Σημειώσεις Στοιχειώδους Θεωρίας Ἀριθμῶν

Ἐαρινὸ ἐξάμηνο 2017-18

Κ. Γκότσης

Οἱ πρόχειρες αυτὲς σημειώσεις ἀπευθύνονται στοὺς φοιτητὲς τοῦ Τμήματος Μαθηματικῶν τοῦ Πανεπιστημίου Ἀθηνῶν, οἱ ὁποῖοι παρακολουθοῦν τὸ μάθημα τῆς Θεωρίας Ἀριθμῶν κατὰ τὸ ἐαρινὸ ἑξάμηνο τοῦ ἀκαδημαϊκοῦ ἔτους 2017-18. Οἱ σημειώσεις αὐτὲς σὲ καμία περίπτωση δὲν μποροῦν νὰ ὑποκαταστήσουν κανένα ἀπὸ τὴν πληθώρα τῶν ἀξιόλογων, σχετικῶν μὲ τὸ ἀντικείμενο, βιβλίων ποὺ ὑπάρχουν στὴ διεθνή βιβλιογραφία, πολλὰ ἀπὸ τὰ ὁποῖα ἔχουν γραφεῖ ἀπὸ τοὺς «μαῖτρ» τοῦ Κλάδου. Γιὰ τὸ λόγο αυτὸ, οἱ παρούσες σημειώσεις δὲν ἀποτελοῦν φυσικὰ πρωτότυπο ἐπιστημονικὸ ἀλλὰ οὔτε καὶ διδακτικὸ ἔργο. Γράφτηκαν ὡς ἕνα εἶδος «ὁδηγοῦ» τοῦ διδάσκοντος καὶ τῶν φοιτητῶν, πρὸς διευκόλυνσή τους κατὰ τὴ διάρκεια τῶν μαθημάτων. Στὶς σημειώσεις αὐτὲς χρησιμοποιήθηκε ὑλικὸ ἀπὸ διάφορα βιβλία. (Κυρίως ἀσκήσεις). Ἀναφέρω τὶς παρακάτω πηγὲς:

- Γιάννης Αντωνιάδης, Αριστείδης Κοντογεώργης, *Θεωρία Αριθμών και εφαρμογές*, σε ηλεκτρονική μορφή, https://repository.kallipos.gr/handle/11419/107
- Δημήτρης Ι. Δεριζιώτης, *Μια εισαγωγή στη Θεωρία Αριθμών*, Β' Έκδοση, Εκδόσεις Σοφία, 2012
- Κώστα Αντώνη Κυριακόπουλου, *Μαθηματικά Β΄ Λυκείου-Θετικής Κατεύθυνσης, Τρίτος Τόμος, Θεωρία Αριθμών*, Εκδόσεις Πατάκη, 1999
- Andrew Adler, John E. Coury, *The Theory of Numbers-A Text and Source Book of Problems*, Jones and Bartlett Publishers, Inc., 1995
- Titu Andreescu, Dorin Andrica, Zuming Feng, *104 Number Theory Problems-From the Training of the USA IMO Team*, Birkhäuser, 2007
- Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976
- David M. Burton, *Elementary Number Theory*, Sixth Edition, McGraw-Hill, 2007
- Anthony A. Gioia, *The Theory of Numbers-An Introduction*, Dover Publications, Inc., 2001
- G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Fifth Edition, Oxford Science Publications, 1979
- Jean-Marie De Koninck, Armel Mercier, *1001 Problems in Classical Number Theory*, American Mathematical Society, 2007

Στὸ τέλος τῶν σημειώσεων προστέθηκαν ἐκτεταμένα μάλλον παραρτήματα, τὰ ὁποῖα σκοπὸ εἶχαν νὰ καλύψουν (ἐν μέρει) τὰ σοβαρὰ κενὰ τῶν πρωτοετῶν κυρίως φοιτητῶν σὲ βασικὰ θέματα, τὰ ὁποῖα διδάσκονταν παλαιότερα στὴ μέση ἐκπαίδευση καὶ τὰ ὁποῖα γιὰ λόγους φτηνοῦ λαϊκισμοῦ, ἀλλὰ καὶ ἄγνοιας ἀφαιρέθηκαν ἀπὸ τὴ διδακτέα ὕλη.

Ἄνοιξη τοῦ 2018,
Κ. Γκότσης

Περιεχόμενα

I Θεωρία ᾽Αριθμῶν

1 Βασικές Έννοιες Διαιρετότητας **9**
- 1.1 Ορισμοί-Ευκλείδειος Διαίρεση . . . 9
- 1.2 Μέγιστος Κοινός Διαιρέτης και Ελάχιστο Κοινό Πολλαπλάσιο . . . 16
- 1.3 Πρώτοι Αριθμοί . . . 28
- 1.4 Η γραμμική διοφαντική εξίσωση $ax+\beta y=\gamma$ . . . 42
- 1.5 Απόδειξη του αιτήματος του Bertrand . . . 46
- 1.6 Λύσεις των ασκήσεων του κεφαλαίου 1 . . . 49

2 Ισοτιμίες και αριθμητικές συναρτήσεις **55**
- 2.1 Ορισμοί-βασικές ιδιότητες . . . 55
- 2.2 Η «περίεργη» αριθμητική modulo n και οι εφαρμογές της σε προβλήματα διαιρετότητας . . . 57
- 2.3 Η συνάρτηση φ του Euler . . . 63
- 2.4 Τα Θεωρήματα των Euler, Fermat και Wilson . . . 68
- 2.5 Επίλυση γραμμικών ισοτιμιών . . . 75
- 2.6 Το Κινεζικό Θεώρημα υπολοίπων . . . 76
- 2.7 Ο δακτύλιος $\mathbb{Z}_n$, όπου $n > 1$ . . . 79
- 2.8 Αριθμητικές συναρτήσεις και ο τύπος αντιστροφής του Möbius . . . 81
- 2.9 Πολυωνυμικές ισοτιμίες . . . 87
- 2.10 Λύσεις των ασκήσεων του κεφαλαίου 2 . . . 87

II Παραρτήματα

Α΄ Σύνολα και συναφείς έννοιες **91**

Β΄ Περί αλγεβρικών δομών-σύντομη επισκόπηση **101**

Γ΄ Τὸ σύνολο $\mathbb{Z}$ τῶν ἀκεραίων ὡς ὑποσύνολο τοῦ συνόλου $\mathbb{R}$ τῶν πραγματικῶν ἀριθμῶν καὶ ἡ μαθηματικὴ ἐπαγωγὴ **109**
- Γ΄.1 «᾽Ολίγα τινὰ» περὶ τῶν ἀκεραίων καὶ ἡ μαθηματικὴ ἐπαγωγὴ . . . 109
- Γ΄.2 Το διώνυμο του Newton . . . 131
- Γ΄.3 Η επαγωγή και οι άλλες αποδεικτικές μέθοδοι . . . 137

Δ΄ Βασικές έννοιες Συνδυαστικής **143**
- Δ΄.1 Η προσθετική και η πολλαπλασιαστική αρχή . . . 143
- Δ΄.2 Διατάξεις-μεταθέσεις . . . 144
- Δ΄.3 Συνδυασμοί . . . 144
- Δ΄.4 Επαναληπτικές διατάξεις-Επαναληπτικοί συνδυασμοί . . . 146
- Δ΄.5 Πολυωνυμικοί συντελεστές . . . 149
- Δ΄.6 Αρχή του εγκλεισμού-αποκλεισμού . . . 150

Μέρος Ι

Θεωρία ᾽Αριθμῶν

Κεφάλαιο 1

Βασικές Έννοιες Διαιρετότητας

1.1 Ορισμοί-Ευκλείδειος Διαίρεση

Ορισμός 1.1. Έστω $\alpha, \beta \in \mathbb{Z}$. Θα λέμε ότι ο $\boldsymbol{\alpha}$ **διαιρεί τον** $\boldsymbol{\beta}$ (ή ότι ο $\boldsymbol{\alpha}$ **είναι διαιρέτης του** $\boldsymbol{\beta}$) ή ισοδύναμα ότι ο $\boldsymbol{\beta}$ **είναι (ακέραιο) πολλαπλάσιο του** $\boldsymbol{\alpha}$ αν και μόνον αν υπάρχει $\lambda \in \mathbb{Z}$ τέτοιο, ώστε $\beta = \lambda\alpha$. Αν ο α διαιρεί τον β, θα γράφουμε $\alpha \mid \beta$. Αν ο α δεν διαιρεί τον β, τότε θα γράφουμε $\alpha \nmid \beta$.

Από τον προηγούμενο ορισμό προκύπτουν άμεσα οι εξής ιδιότητες:

Πρόταση 1.2. **(i)** $\alpha \mid 0$, $\pm\alpha \mid \alpha$ και $\alpha \mid \pm\alpha$, για κάθε $\alpha \in \mathbb{Z}$.
(ii) $\pm 1 \mid \alpha$ για κάθε $\alpha \in \mathbb{Z}$.
(iii) Αν $\alpha \mid \beta$ και $\beta \mid \gamma$, τότε $\alpha \mid \gamma$.
(iv) Αν $\alpha \mid \beta$ και $\alpha \mid \gamma$, τότε $\alpha \mid \beta \pm \gamma$. Γενικότερα, αν $\alpha \mid \beta_i$ για κάθε $i = 1, 2, \ldots, n$, τότε $\alpha \mid \sum_{i=1}^{n} \mu_i\beta_i$, για κάθε $\mu_1, \mu_2, \ldots, \ldots \mu_n \in \mathbb{Z}$.
(v) Αν $\beta \mid \gamma$ και $\alpha \in \mathbb{Z}$, τότε $\alpha\beta \mid \alpha\gamma$. Αν $\alpha \neq 0$, τότε ισχύει η ισοδυναμία: $\beta \mid \gamma \Leftrightarrow \alpha\beta \mid \alpha\gamma$.
(vi) Αν $\alpha_1 \mid \beta_1, \alpha_2 \mid \beta_2, \ldots, \alpha_n \mid \beta_n$, τότε $\alpha_1\alpha_2\cdots\alpha_n \mid \beta_1\beta_2\cdots\beta_n$. Στην περίπτωση που $\alpha_1 = \alpha_2 = \cdots = \alpha_n = \alpha$ και $\beta_1 = \beta_2 = \cdots = \beta_n = \beta$ παίρνουμε: $\alpha \mid \beta \Rightarrow \alpha^n \mid \beta^n$.
(vii) Ισχύει η ισοδυναμία: $0 \mid \alpha \Leftrightarrow \alpha = 0$.
(viii) Αν $\alpha \neq 0$, τότε ισχύει η ισοδυναμία: $\alpha \mid \beta \Leftrightarrow \dfrac{\beta}{\alpha} \in \mathbb{Z}$.
(ix) Αν $\alpha \mid \beta$ και $\beta \neq 0$, τότε $|\alpha| \leq |\beta|$. Συνεπώς αν $\alpha \mid \beta$ και $\beta \mid \alpha$, τότε $|\alpha| = |\beta|$. Επίσης, αν $\alpha \mid 1$, τότε $\alpha = \pm 1$.
(x) Αν $\alpha \mid \beta$ και $\alpha \neq 0$, τότε και $\dfrac{\beta}{\alpha} \;\Big|\; \beta$.
(xi) Αν $\alpha \mid \beta$, $\gamma \neq 0$, $\gamma \mid \alpha$ και $\gamma \mid \beta$, τότε $\dfrac{\alpha}{\gamma} \;\Big|\; \dfrac{\beta}{\gamma}$.

Απόδειξη: (i) $0 = 0 \cdot \alpha$, $\alpha = 1 \cdot \alpha = (-1)(-\alpha)$ και $-\alpha = (-1)\alpha$, για κάθε $\alpha \in \mathbb{Z}$.
(ii) $\alpha = \alpha \cdot 1 = (-\alpha)(-1)$.
(iii) Εφόσον $\alpha \mid \beta$ και $\beta \mid \gamma$, θα έχουμε $\beta = \lambda \cdot \alpha$ και $\gamma = \lambda' \cdot \beta$, όπου $\lambda, \lambda' \in \mathbb{Z}$. Επομένως $\gamma = (\lambda\lambda') \cdot \alpha$ και προφανώς $\lambda\lambda' \in \mathbb{Z}$.
(iv) $\alpha \mid \beta_i \Leftrightarrow \beta_i = \lambda_i \cdot \alpha$, όπου $\lambda_i \in \mathbb{Z}$ για κάθε $i = 1, 2, \ldots, n$. Επομένως $\sum_{i=1}^{n} \mu_i\beta_i = \left(\sum_{i=1}^{n} \mu_i\lambda_i\right)\alpha = \lambda\alpha$, όπου $\lambda = \sum_{i=1}^{n} \mu_i\lambda_i \in \mathbb{Z}$.
(v) $\beta \mid \gamma \Leftrightarrow \gamma = \lambda\beta$, όπου $\lambda \in \mathbb{Z}$. Άρα $\alpha\gamma = \lambda \cdot (\alpha\beta) \Rightarrow \alpha\beta \mid \alpha\gamma$. Αν τώρα $\alpha \neq 0$, τότε η σχέση $\alpha\gamma = \lambda\alpha\beta$, όπου $\lambda \in \mathbb{Z}$, είναι ισοδύναμη με τη σχέση $\alpha(\gamma - \lambda\beta) = 0 \underset{\alpha\neq 0}{\Leftrightarrow} \gamma = \lambda\beta \Leftrightarrow \beta \mid \gamma$.
(vi) Έστω Αν $\alpha_1 \mid \beta_1, \alpha_2 \mid \beta_2, \ldots, \alpha_n \mid \beta_n$. Τότε υπάρχουν $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Z}$ τέτοια, ώστε $\beta_i = \lambda_i\alpha_i$, για κάθε $i = 1, 2, \ldots, n$. Επομένως $\alpha_1\alpha_2\cdots\alpha_n = (\lambda_1\lambda_2\cdots\lambda_n)\beta_1\beta_2\cdots\beta_n$. Άρα $\beta_1\beta_2\cdots\beta_n \mid \alpha_1\alpha_2\cdots\alpha_n$.
(vii) Έστω $0 \mid \alpha$. Τότε υπάρχει $\lambda \in \mathbb{Z}$ τέτοιο, ώστε $\alpha = \lambda \cdot 0 = 0$. Αντιστρόφως, $0 = \lambda \cdot 0$, για κάθε $\lambda \in \mathbb{Z}$ και κατά συνέπεια $0 \mid 0$.

(viii) Έστω $\alpha \neq 0$ και $\alpha \mid \beta$. Τότε υπάρχει $\lambda \in \mathbb{Z}$ τέτοιο, ώστε $\beta = \lambda\alpha \underset{\alpha\neq 0}{\Leftrightarrow} \dfrac{\beta}{\alpha} = \lambda \in \mathbb{Z}$. Αντιστρόφως, αν $\lambda := \dfrac{\beta}{\alpha} \in \mathbb{Z}$, τότε $\beta = \lambda\alpha \Rightarrow \alpha \mid \beta$.

(ix) Από το **(vii)** προκύπτει ότι και $\alpha \neq 0$. Από το **(viii)**, επειδή $\alpha, \beta \neq 0$, έπεται ότι $\dfrac{\beta}{\alpha} \in \mathbb{Z} \setminus \{0\}$. Επομένως $\left|\dfrac{\beta}{\alpha}\right| \geq 1 \Leftrightarrow |\alpha| \leq |\beta|$.

(x) Έστω $\alpha \neq 0$ και $\alpha \mid \beta$. Τότε ο αριθμός $\lambda = \dfrac{\beta}{\alpha}$ είναι ακέραιος. Προφανώς $\beta = \alpha \cdot \dfrac{\beta}{\alpha}$ και κατά συνέπεια $\dfrac{\beta}{\alpha} \,\Big|\, \beta$.

(xi) Εφόσον $\gamma \neq 0$, $\gamma \mid \alpha$ και $\gamma \mid \beta$, οι αριθμοί $\dfrac{\alpha}{\gamma}$ και $\dfrac{\beta}{\gamma}$ είναι ακέραιοι. Τώρα, επειδή $\alpha \mid \beta$, υπάρχει $\lambda \in \mathbb{Z}$ τέτοιο, ώστε $\beta = \lambda\alpha \Leftrightarrow \dfrac{\beta}{\gamma} = \lambda \cdot \dfrac{\alpha}{\gamma}$, δηλαδή $\dfrac{\alpha}{\gamma} \,\Big|\, \dfrac{\beta}{\gamma}$. ■

Παρατηρήσεις: 1) Λόγω της ισοδυναμίας $0 \mid \alpha \Leftrightarrow \alpha = 0$ (**(vii)** προηγούμενης πρότασης), η περίπτωση του μηδενικού διαιρέτη δεν παρουσιάζει ενδιαφέρον. Γι' αυτό στα επόμενα, όταν γράφουμε $\alpha \mid \beta$ θα θεωρούμε ότι $\alpha \neq 0$, εκτός αν άλλως τονίζεται.
2) Από το **(ix)** της προηγούμενης πρότασης προκύπτει ότι αν οι ακέραιοι α, β είναι ομόσημοι, τότε ένας τρόπος για να δείξουμε ότι $\alpha = \beta$ είναι να δείξουμε ότι $\alpha \mid \beta$ και $\beta \mid \alpha$. Τη μέθοδο αυτή θα χρησιμοποιούμε αρκετά συχνά στα επόμενα.

Θεώρημα 1.3. (Ταυτότητα της Ευκλειδείου Διαιρέσεως) Έστω $\alpha, \beta \in \mathbb{Z}$ με $\beta \neq 0$. Τότε υπάρχουν **μοναδικοί** ακέραιοι π και υ τέτοιοι, ώστε

$$\alpha = \beta\pi + \upsilon,$$

με $0 \leq \upsilon < |\beta|$.
Απόδειξη: (Ύπαρξη) Έστω $A = \{\alpha - \beta x \mid x \in \mathbb{Z} \text{ και } \alpha - \beta x \geq 0\}$. Κατ' αρχάς θα αποδείξουμε ότι το $A \subseteq \mathbb{Z}$ είναι μη κενό. Εφόσον $\beta \neq 0$, $|\beta| \geq 1 \Leftrightarrow \beta^2 \geq 1$. Παρατηρούμε ότι για $x = -\beta|\alpha|$ έχουμε $\alpha - \beta x = \alpha + \beta^2|\alpha| \geq \alpha + |\alpha| \geq 0$. Άρα $A \neq \varnothing$. Το A είναι προφανώς κάτω φραγμένο από το μηδέν και κατά συνέπεια, περιέχει (μοναδικό) ελάχιστο στοιχείο το οποίο συμβολίζουμε με υ. Επομένως $0 \leq \upsilon = \alpha - \beta\pi$, για κάποιο $\pi \in \mathbb{Z}$. Απομένει να δειχθεί ότι $\upsilon < |\beta|$.
Υποθέτουμε λοιπόν $\upsilon \geq |\beta|$. Αν $\epsilon = \pm 1$ είναι το πρόσημο του β, δηλαδή $\epsilon = -1$ αν $\beta < 0$ και $\epsilon = 1$ αν $\beta > 0$, τότε $|\beta| = \epsilon\beta$. Τότε ο ακέραιος $\upsilon' = \upsilon - |\beta|$ είναι μη αρνητικός (από υπόθεση) και μικρότερος του υ. Αλλά $\upsilon' = \upsilon - |\beta| = \alpha - \beta\pi - \epsilon\beta = \alpha - \beta(\pi + \epsilon)$, ήτοι της μορφής $\alpha - \beta x$. Επομένως το υ' είναι στοιχείο του A, άτοπο γιατί το υ είναι το ελάχιστο στοιχείο του A και $\upsilon' < \upsilon$.
(Μοναδικότητα) Έστω $\pi_1, \upsilon_1 \in \mathbb{Z}$ τέτοιοι, ώστε $\alpha = \beta\pi_1 + \upsilon_1$, με $0 \leq \upsilon_1 < |\beta|$. Αφαιρούμε τις σχέσεις $\alpha = \beta\pi + \upsilon$ και $\alpha = \beta\pi_1 + \upsilon_1$ κατά μέλη και παίρνουμε: $0 = \beta(\pi - \pi_1) + \upsilon - \upsilon_1 \Leftrightarrow \upsilon - \upsilon_1 = \beta(\pi_1 - \pi) \Rightarrow$
$\Rightarrow |\upsilon - \upsilon_1| = |\beta||\pi - \pi_1|$.
Υποθέτουμε ότι $\pi \neq \pi_1 \Leftrightarrow |\pi - \pi_1| \geq 1 \Rightarrow |\upsilon - \upsilon_1| = |\beta||\pi - \pi_1| \geq |\beta|$. Αλλά,

$$\left.\begin{array}{r} 0 \leq \upsilon < |\beta| \\ 0 \leq \upsilon_1 < |\beta| \quad \Leftrightarrow -|\beta| < -\upsilon_1 \leq 0 \end{array}\right\} \Rightarrow -|\beta| < \upsilon - \upsilon_1 < |\beta| \Leftrightarrow |\upsilon - \upsilon_1| < |\beta|, \text{ αντίφαση.}$$

Επομένως $\pi = \pi_1$ και συνεπώς $\upsilon = \upsilon_1$. ■

Από την ταυτότητα της ευκλειδείου διαιρέσεως προκύπτει η σχέση $\dfrac{\alpha}{\beta} = \pi + \dfrac{\upsilon}{\beta}$. Αν $\beta > 0$, τότε $\pi \leq \pi + \dfrac{\upsilon}{\beta} \underset{\upsilon<\beta}{<} \pi + 1$, ήτοι $\pi \leq \dfrac{\alpha}{\beta} < \pi + 1$. Επομένως $\pi = \left\lfloor \dfrac{\alpha}{\beta} \right\rfloor$, το ακέραιο μέρος του $\dfrac{\alpha}{\beta}$, δηλαδή ο μεγαλύτερος ακέραιος που δεν υπερβαίνει το $\dfrac{\alpha}{\beta}$. Αν τώρα $\beta < 0$, τότε επειδή $0 \leq \upsilon < |\beta| = -\beta$, έχουμε $0 \geq \dfrac{\upsilon}{\beta} > -1$. Επομένως $\pi \geq \pi + \dfrac{\upsilon}{\beta} = \dfrac{\alpha}{\beta} > \pi - 1$, ήτοι $\pi = \left\lceil \dfrac{\alpha}{\beta} \right\rceil$, ο μικρότερος ακέραιος που δεν υπολείπεται του $\dfrac{\alpha}{\beta}$.

Από το προηγούμενο θεώρημα συνάγουμε επίσης τα ακόλουθα συμπεράσματα:
Οι ακέραιοι αριθμοί χωρίζονται σε δύο ξεχωριστές κλάσεις. Η μία αποτελείται από τους αριθμούς της μορφής 2π, $\pi \in \mathbb{Z}$ που ονομάζονται **άρτιοι** και οι άλλοι από τους αριθμούς της μορφής $2\pi+1$, $\pi \in \mathbb{Z}$ που ονομάζονται **περιττοί**. Από τη μοναδικότητα των π και υ δεν μπορεί ένας ακέραιος να είναι ταυτόχρονα άρτιος και περιττός.
Ομοίως, υπάρχουν τρεις ξένες μεταξύ τους κλάσεις στις οποίες χωρίζονται οι ακέραιοι, ανάλογα με το υπόλοιπο που δίνουν όταν διαιρεθούν με το 3. Αυτές είναι οι $\{3\pi \mid \pi \in \mathbb{Z}\}$, $\{3\pi+1 \mid \pi \in \mathbb{Z}\}$ και $\{3\pi+2 \mid \pi \in \mathbb{Z}\}$. Φυσικά το σύμβολο π μπορεί να αντικατασταθεί από οποιοδήποτε άλλο, πχ. k, r, t κτλ. Η διάκριση αυτών των περιπτώσεων εφαρμόζεται πολύ συχνά σε ασκήσεις, προκειμένου να δείξουμε ότι ένας ακέραιος διαιρεί μια παράσταση. Για παράδειγμα, ας δούμε το εξής στοιχειώδες αποτέλεσμα:

Παράδειγμα 1.4. **(i)** Για κάθε ακέραιο n ο αριθμός $n(n+1)$ είναι άρτιος.
(ii) Το τετράγωνο ενός περιττού διαιρούμενο με το 8 δίνει υπόλοιπο 1.
(iii) Το τετράγωνο ενός μη πολλαπλασίου του 3, διαιρούμενο με το 3, δίνει υπόλοιπο 1.
(iv) Το τετράγωνο ενός μη πολλαπλασίου του 5, διαιρούμενο με το 5, δίνει υπόλοιπο 1 ή 4.
Απόδειξη: **(i)** Διακρίνουμε δύο περιπτώσεις: **α)** $n = 2k$, άρτιος. Τότε $n(n+1) = 2(k(2k+1))$, ήτοι πολλαπλάσιο του 2. **β)** $n = 2k+1$, περιττός. Τότε $n+1 = 2k+2 = 2(k+1)$, άρτιος. Επομένως $n(n+1) = 2((k+1)(2k+1))$, άρτιος και πάλι.
(ii) Ένας περιττός είναι της μορφής $2k+1$. Παρατηρούμε ότι $(2k+1)^2 = 4k^2+4k+1 = 4k(k+1)+1$. Σύμφωνα με το **(i)**, ο $k(k+1)$ είναι πολλαπλάσιο του 2 και άρα ο $4k(k+1)$ είναι πολλαπλάσιο του 8. Αν γράψουμε τον $4k(k+1)$ στη μορφή 8λ, παίρνουμε $(2k+1)^2 = 8\lambda+1$.
(iii) Ένα μη πολλαπλάσιο του 3 είναι της μορφής $3k+1$ ή $3k+2$. Παρατηρούμε ότι $(3k+1)^2 = 9k^2+6k+1 = 3k(3k+2)+1$ και $(3k+2)^2 = 9k^2+12k+4 = 9k^2+12k+3+1 = 3(3k^2+4k+1)+1$.
(iv) Ένα μη πολλαπλάσιο του 5 είναι της μορφής **α)** $5k+1$ ή **β)** $5k+2$ ή **γ)** $5k+3$ ή **δ)** $5k+4$. Παρατηρούμε ότι:
α) $(5k+1)^2 = 25k^2+10k+1 = 5k(5k+2)+1$,
β) $(5k+2)^2 = 25k^2+20k+4 = 5k(5k+4)+4$,
γ) $(5k+3)^2 = 25k^2+30k+9 = 25k^2+30k+5+4 = 5(5k^2+6k+1)+4$ και τέλος,
δ) $(5k+4)^2 = 25k^2+40k+16 = 25k^2+40k+15+1 = 5(5k^2+8k+3)+1$. ■

Η διάκριση των ακεραίων σε κλάσεις, ανάλογα με το υπόλοιπο που δίνουν όταν διαιρεθούν από έναν ακέραιο ≥ 2 αποτελεί ενδιαφέρον αντικείμενο της Θεωρίας Αριθμών, στο οποίο θα επανέλθουμε αργότερα.

ΛΥΜΕΝΕΣ ΑΣΚΗΣΕΙΣ

Άσκηση 1. Δείξτε ότι αν $n = 4k+1$, όπου $k \in \mathbb{Z}$, τότε $4 | n^3+2n+1$.
Απόδειξη: $n^3+2n+1 = (4k+1)^3+2(4k+1)+1 = 64k^3+48k^2+12k+1+8k+2+1 = 4(16k^3+12k^2+ +5k+1)$. ■

Άσκηση 2. **(i)** Το άθροισμα αρτίου πλήθους περιττών είναι άρτιος, ενώ το άθροισμα περιττού πλήθους περιττών είναι περιττός.
(ii) Το γινόμενο περιττών είναι περιττός.
Απόδειξη: **(i)** Έστω n περιττοί αριθμοί $\alpha_1 = 2k_1+1, \alpha_2 = 2k_2+1, \ldots, \alpha_n = 2k_n+1$. Τότε $\alpha_1+\alpha_2\cdots+\alpha_n = = 2(k_1+k_2+\cdots+k_n)+n = 2k+n$, όπου $k = k_1+k_2+\cdots+k_n$.
Αν λοιπόν $n = 2m$ άρτιος, τότε $\alpha_1+\alpha_2\cdots+\alpha_n = 2(k+m)$ άρτιος.
Αν $n = 2m+1$ περιττός, τότε $\alpha_1+\alpha_2\cdots+\alpha_n = 2(k+m)+1$ περιττός.
(ii) Θα αποδείξουμε την πρόταση πρώτα για δύο περιττούς. Έστω $\alpha_1 = 2k_1+1$ και $\alpha_2 = 2k_2+1$ περιττοί. Τότε $\alpha_1\alpha_2 = (2k_1+1)(2k_2+1) = 2(2k_1k_2+k_1+k_2)+1 = 2\lambda+1$, όπου $\lambda = 2k_1k_2+k_1+k_2$. Έστω τώρα $n > 2$ περιττοί αριθμοί $\alpha_1, \alpha_2, \ldots, \alpha_n$. Με επαγωγή επί του n υποθέτουμε ότι το γινόμενο $\alpha_1\alpha_2\cdots\alpha_{n-1}$ είναι περιττός. Τότε, εφόσον ο ισχυρισμός ισχύει για $n = 2$, το γινόμενο $\alpha_1\alpha_2\cdots\alpha_{n-1}\alpha_n = (\alpha_1\alpha_2\cdots\alpha_{n-1})\alpha_n$ είναι περιττός. ■

Άσκηση 3. Για κάθε $\lambda \in \mathbb{Z}$ ο αριθμός $\lambda(\lambda^2+2)$ είναι πολλαπλάσιο του 3.
Απόδειξη: Κατ' αρχάς, αν $3 \mid \lambda$, τότε $3 \mid \lambda(\lambda^2+2)$. Έστω τώρα ότι $3 \nmid \lambda$. Τότε ο αριθμός λ^2, αν διαιρεθεί με το 3 δίνει υπόλοιπο 1. Πράγματι, έστω $\lambda = 3\kappa+1$, $\kappa \in \mathbb{Z}$. Τότε $\lambda^2 = 9\kappa^2+6\kappa+1 = 3\kappa(3\kappa+2)+1$. Αν $\lambda = 3\kappa+2$, $\kappa \in \mathbb{Z}$, τότε $\lambda^2 = 9\kappa^2+12\kappa+4 = 3(3\kappa^2+4\kappa+1)+1$. Σε κάθε περίπτωση, αν $3 \nmid \lambda$, τότε $\lambda^2 = 3\mu+1$, όπου $\mu \in \mathbb{Z}$. Επομένως $\lambda^2+2 = 3\mu+3 = 3(\mu+1)$, ήτοι $3 \mid \lambda^2+2$ και επομένως $3 \mid \lambda(\lambda^2+2)$. ■

Άσκηση 4. Αν $n \geq 1$ είναι περιττός ακέραιος, τότε $16 \mid n^4+4n^2+11$.
Απόδειξη: Κατ' αρχάς, από το (ii) του παραδείγματος 1.4 έχουμε ότι το τετράγωνο περιττού είναι της μορφής $8\lambda+1$. Επομένως, αν από τετράγωνο περιττού αφαιρέσουμε το 1, ο αριθμός που θα προκύψει είναι πολλαπλάσιο του 8. Έχουμε: $n^4+4n^2+11 = n^4-1+4(n^2-1)+16 = (n^2-1)(n^2+1)+4(n^2-1)+16$. Ο n^2-1 διαιρείται με το 8 και ο n^2+1 είναι άρτιος (ως άθροισμα περιττών) και συνεπώς διαιρείται με το 2. Άρα ο $(n^2-1)(n^2+1)$ διαιρείται με το 16. Επειδή ο n^2-1 διαιρείται με το 8, ο $4(n^2-1)$ διαιρείται με το 32, άρα και με το 16. Τέλος, ο 16 διαιρείται από τον εαυτό του. Άρα ο $n^4+4n^2+11 = (n^2-1)(n^2+1)+4(n^2-1)+16$ είναι πολλαπλάσιο του 16. ■

Άσκηση 5. Για κάθε $\alpha \in \mathbb{Z}$ ο αριθμός $3\alpha^2-1$ δεν είναι τέλειο τετράγωνο (τετράγωνο ακεραίου).
Απόδειξη: Έστω $3\alpha^2-1 = x^2 \Leftrightarrow 3\alpha^2 = x^2+1 \Rightarrow 3 \mid x^2+1$. Αν $x = 3k$, τότε $3 \mid 9k^2+1 \underset{3|9k^2}{\Rightarrow} 3 \mid 1$, άτοπο. Αν $x = 3k+1$ ή $x = 3k+2$, τότε, όπως είδαμε στο παράδειγμα 1.4 (iii), το x^2 είναι της μορφής $3\mu+1$, $\mu \in \mathbb{Z}$. Άρα $3\alpha^2 = x^2+1 = 3\mu+2 \underset{3|3\mu}{\Rightarrow} 3 \mid 2$, άτοπο. ■

Άσκηση 6. Αν $\alpha \neq \beta$ και $(\alpha-\beta) \mid (\alpha x+\beta y)$, τότε $(\alpha-\beta) \mid (\alpha y+\beta x)$.
Απόδειξη: $(\alpha y+\beta x)-(\alpha x+\beta y) = \alpha y-\alpha x+\beta x-\beta y = \alpha(y-x)-\beta(y-x) = (\alpha-\beta)(y-x)$, ήτοι $(\alpha-\beta) \mid (\alpha y+\beta x)-(\alpha x+\beta y)$. Επειδή $(\alpha-\beta) \mid (\alpha x+\beta y)$, παίρνουμε $(\alpha-\beta) \mid (\alpha y+\beta x)-(\alpha x+\beta y)+$ $+(\alpha x+\beta y) = \alpha y+\beta x$. ■

Άσκηση 7. Αν $n = 0, 1, 2, \ldots$, τότε $9 \mid 2^{4n+1}-2^{2n}-1$.
Απόδειξη: Θέτουμε $x = 2^{2n}$. Τότε $2^{4n+1}-2^{2n}-1 = 2x^2-x-1 = x^2-x+x^2-1 = x(x-1)+(x+1)(x-1) =$ $= (x-1)(2x+1)$. Παρατηρούμε ότι: $x-1 = 2^{2n}-1 = 4^n-1 = (4-1)(4^{n-1}+4^{n-2}+\cdots+1) = 3k$, όπου $k = 4^{n-1}+4^{n-2}+\cdots+1$. Επίσης, $2x+1 = 2^{2n+1}+1 = (2+1)(2^{2n}-2^{2n-1}+2^{2n-2}-\cdots+1) = 3r$, όπου $r = 2^{2n}-2^{2n-1}+2^{2n-2}-\cdots+1$. Επομένως $2^{4n+1}-2^{2n}-1 = (x-1)(2x+1) = 9kr$. ■

Άσκηση 8. Αν $k, r \in \mathbb{Z}$ τέτοιοι ώστε $4k+1 = 3r$, να βρεθεί ο γενικός τύπος του k.
Λύση: Η σχέση $4k+1 = 3r$ είναι ισοδύναμη με τη σχέση $3 \mid 4k+1$. Διακρίνουμε περιπτώσεις: **(i)** $k = 3s$, **(ii)** $k = 3s+1$ και **(iii)** $k = 3s+2$, όπου $s \in \mathbb{Z}$. Στην πρώτη περίπτωση παίρνουμε $12s+1 = 3r \Leftrightarrow 3(r-4s) = 1$, ήτοι $3 \mid 1$, άτοπο. Στη δεύτερη περίπτωση παίρνουμε $12s+5 = 3r \Leftrightarrow 3(r-4s) = 5$, ήτοι $3 \mid 5$, άτοπο. Στην τελευταία περίπτωση παίρνουμε $12s+9 = 3r \Leftrightarrow 4s+3 = r$. Άρα $k = 3s+2$ και $r = 4s+3$, όπου $s \in \mathbb{Z}$. ■

Άσκηση 9. Αν n είναι θετικός ακέραιος, τότε ο αριθμός n^2+n+1 δεν είναι τετράγωνο ακεραίου.
Απόδειξη: Παρατηρούμε ότι $n^2 < n^2+n+1 < n^2+2n+1 = (n+1)^2$. Αν λοιπόν $n^2+n+1 = k^2$, όπου $k > 0$, τότε θα έπρεπε $n^2 < k^2 < (n+1)^2 \Leftrightarrow n < k < n+1$, άτοπο. ■

Άσκηση 10. Για κάθε φυσικό αριθμό n ισχύουν οι σχέσεις:
(i) $5 \mid 3^{3n+2}+2^{n+4}$, **(ii)** $7 \mid 3^{2n+1}+2^{n+2}$, **(iii)** $11 \mid 3^{2n+2}+2^{6n+1}$ και **(iv)** $29 \mid 17^{2n+1}+12(-1)^n$.
Απόδειξη: Θα εφαρμόσουμε επαγωγή επί του n και για τις τέσσερις σχέσεις. Η περίπτωση $n = 0$ αποτελεί αριθμητική εφαρμογή, την οποία ο αναγνώστης μπορεί να επαληθεύσει άμεσα. Θα ασχοληθούμε με τα επαγωγικά βήματα.
(i) Έστω $5 \mid 3^{3n+2}+2^{n+4}$, δηλαδή $3^{3n+2}+2^{n+4} = 5\lambda$, όπου $\lambda \in \mathbb{Z}$. Θα δείξουμε ότι $5 \mid 3^{3n+5}+2^{n+5}$. Έχουμε: $3^{3n+5}+2^{n+5} = 27 \cdot 3^{3n+2}+2 \cdot 2^{n+4} = 25 \cdot 3^{3n+2}+2(3^{3n+2}+2^{n+4}) = 25 \cdot 3^{3n+2}+2 \cdot 5\lambda = 5 \cdot (5 \cdot 3^{3n+2}+2\lambda)$.
(ii) Υποθέτουμε ότι $3^{2n+1}+2^{n+2} = 7\lambda$, $\lambda \in \mathbb{Z}$. Τότε, $3^{2n+3}+2^{n+3} = 9 \cdot 3^{2n+1}+2 \cdot 2^{n+2} = 7 \cdot 3^{2n+1}+2 \cdot (3^{2n+1}+2^{n+2}) = 7 \cdot 3^{2n+1}+14\lambda = 7 \cdot (3^{2n+1}+2\lambda)$.

(iii) Υποθέτουμε ότι $3^{2n+2}+2^{6n+1}=11\lambda$, $\lambda\in\mathbb{Z}$. Τότε, $3^{2n+4}+2^{6n+7}=9\cdot 3^{2n+2}+64\cdot 2^{6n+1}=11\cdot(3^{2n+2}+$ $+6\cdot 2^{6n+1})-2\cdot(3^{2n+2}+2^{6n+1})=11\cdot(3^{2n+2}+6\cdot 2^{6n+1}-2\lambda)$.
(iv) Έστω ότι $29\mid 17^{2n+1}+12(-1)^n$. Τότε $17^{2n+1}+12(-1)^n=29\lambda$, όπου $\lambda\in\mathbb{Z}$. Για $n+1$ έχουμε: $17^{2(n+1)+1}+12(-1)^{(n+1)}=17^2\cdot 17^{2n+1}-12(-1)^n=289\cdot 17^{2n+1}-12(-1)^n=(290-1)\cdot 17^{2n+1}-12(-1)^n=$ $=29\cdot 10\cdot 17^{2n+1}-17^{2n+1}-12(-1)^n=29\cdot 10\cdot 17^{2n+1}-(17^{2n+1}+12(-1)^n)=29\cdot 10\cdot 17^{2n+1}-29\lambda=$ $=29\cdot(10\cdot 17^{2n+1}-\lambda)$. ■

Άσκηση 11. Θεωρούμε την ακολουθία $\alpha_1=1$, $\alpha_2=11$, $\alpha_3=111$, …, $\alpha_n=\underbrace{111\cdots 1}_{n\text{ μονάδες}}$, … Να αποδείξετε ότι για κάθε $n\geq 2$ ο αριθμός α_n δεν είναι τέλειο τετράγωνο.
Απόδειξη: Κατ' αρχάς παρατηρούμε ότι όλοι οι όροι της παραπάνω ακολουθίας είναι περιττοί. Αν λοιπόν $\alpha_n=x^2$, για κάποιο θετικό ακέραιο x, τότε ο x θα ήταν περιττός. (Τετράγωνο αρτίου είναι άρτιος). Επίσης, αν $n\geq 2$, τότε $\alpha_n-1=\underbrace{111\cdots 1}_{n\text{ μονάδες}}-1=\underbrace{111\cdots 1}_{n-1\text{ μονάδες}}0=10\cdot\underbrace{111\cdots 1}_{n-1\text{ μονάδες}}=10\alpha_{n-1}$. Αν λοιπόν $\alpha_n=x^2$, τότε $\alpha_n-1=x^2-1=(x-1)(x+1)\Leftrightarrow 10\alpha_{n-1}=(x-1)(x+1)$. Εφόσον x περιττός, οι αριθμοί $x-1$ και $x+1$ είναι άρτιοι. Έστω $x-1=2k$ και $x+1=2r$. Τότε $(x-1)(x+1)=4kr$, δηλαδή $10\alpha_{n-1}=4kr\Leftrightarrow 5\alpha_{n-1}=2kr\Rightarrow 2\mid 5\alpha_{n-1}$, άτοπο γιατί οι αριθμοί 5 και α_{n-1} είναι περιττοί, άρα και το γινόμενό τους περιττό. ■

Θυμίζουμε ότι για n φυσικό, το $n!$ (n-παραγοντικό) ορίζεται ως εξής: $n!=\begin{cases}1, & \text{αν } n=0\\ 1\cdot 2\cdot 3\cdots n, & \text{αν } n>0\end{cases}$

Άσκηση 12. Για κάθε θετικό ακέραιο n να δείξετε (χωρίς τη χρήση διωνυμικών συντελεστών) ότι το $n!$ διαιρεί το γινόμενο n διαδοχικών ακεραίων.
Απόδειξη: Αν κάποιος από τους n διαδοχικούς ακεραίους είναι μηδέν, τότε και το γινόμενό τους είναι μηδέν και άρα διαιρείται από το $n!$. Αν πάλι όλοι οι διαδοχικοί ακέραιοι είναι αρνητικοί της μορφής $-k,-k-1,-k-2,\ldots,-k-n+1$, όπου $k>0$, τότε το γινόμενό τους ισούται με $(-k)(-k-1)(-k-$ $-2)\cdots(-k-n+1)=(-1)^n k(k+1)(k+2)\cdots(k+n-1)$. Επομένως το πρόβλημα ανάγεται στο να αποδειχθεί ότι το $n!$ διαιρεί το γινόμενο n διαδοχικών θετικών ακεραίων. Εφαρμόζουμε επαγωγή επί του n. Για $n=1$ έχουμε $n!=1$ και η περίπτωση είναι τετριμμένη. Υποθέτουμε ότι το $n!$ διαιρεί κάθε γινόμενο της μορφής $k(k+1)(k+2)\cdots(k+n-1)$, όπου $k>0$. Θα αποδείξουμε ότι το $(n+1)!$ διαιρεί κάθε γινόμενο $n+1$ διαδοχικών ακεραίων. Ένα τέτοιο γινόμενο είναι της μορφής $k(k+1)(k+2)\cdots(k+n-1)(k+n)$. Εδώ εφαρμόζουμε δεύτερη επαγωγή επί του $k>0$.
Για $k=1$ παίρνουμε το γινόμενο $1\cdot 2\cdot 3\cdots(n+1)=(n+1)!$, το οποίο διαιρείται προφανώς από τον εαυτό του. Υποθέτουμε ότι $(n+1)!\mid k(k+1)(k+2)\cdots(k+n-1)(k+n)$, για κάποιο $k>0$. Θα αποδείξουμε ότι $(n+1)!\mid(k+1)(k+2)(k+3)\cdots(k+n)(k+n+1)$. Παρατηρούμε ότι $(k+1)(k+2)(k+3)\cdots(k+n)(k+$ $+n+1)-k(k+1)(k+2)\cdots(k+n-1)(k+n)=(k+1)(k+2)\cdots(k+n)(k+n+1-k)=(k+1)(k+2)\cdots(k+$ $+n)(n+1)=\lambda n!(n+1)=\lambda(n+1)!$, γιατί υποθέσαμε ότι το $n!$ διαιρεί το γινόμενο $(k+1)(k+2)\cdots(k+n)$ από n διαδοχικούς ακέραιους, και άρα $(k+1)(k+2)\cdots(k+n)=\lambda n!$, όπου $\lambda\in\mathbb{Z}$. Κατά συνέπεια το $(n+1)!$ διαιρεί τη διαφορά $(k+1)(k+2)(k+3)\cdots(k+n)(k+n+1)-k(k+1)(k+2)\cdots(k+n-1)(k+n)$ και επειδή $(n+1)!\mid k(k+1)(k+2)\cdots(k+n-1)(k+n)$, έπεται ότι $(n+1)!\mid(k+1)(k+2)(k+3)\cdots(k+n)(k+n+1)$. Η απόδειξη είναι τώρα πλήρης. ■

Άσκηση 13. Για κάθε ακέραιο $n\geq 0$, δείξτε ότι $\dfrac{(3n)!}{(3!)^n}\in\mathbb{Z}$.
Απόδειξη: Πρέπει να δείξουμε ότι $6^n\mid(3n)!$ Για $n=0$ έχουμε $1\mid 0!=1$ που ισχύει. Έστω ότι $6^n\mid(3n)!$ και $\lambda=\dfrac{(3n)!}{6^n}$. Τότε $(3(n+1))!=(3n+3)!=(3n+3)(3n+2)(3n+1)(3n)!=\lambda\cdot 6^n\cdot(3n+1)(3n+2)(3n+3)$. Σύμφωνα με την προηγούμενη άσκηση το $6=3!$ διαιρεί το γινόμενο των τριών διαδοχικών ακεραίων $3n+1$, $3n+2$ και $3n+3$. Έστω $\mu=\dfrac{(3n+1)(3n+2)(3n+3)}{6}$. Συνεπώς $(3(n+1))!=\lambda\mu\cdot 6^{n+1}$. ■

Άσκηση 14. Να αποδείξετε ότι $2^n\mid(n+1)(n+2)(n+3)\cdots(2n)$.
Απόδειξη: Θα αποδείξουμε κάτι ισχυρότερο: ότι η μεγαλύτερη δύναμη του 2 που διαιρεί το $(n+1)(n+$

$+2)(n+3)\cdots(2n)$ είναι το 2^n. Έστω $\mathrm{A}_n=(n+1)(n+2)(n+3)\cdots(2n)$. Τότε έχουμε: $\mathrm{A}_n=(n+1)(n+2)(n+3)\cdots(2n)=2\cdot(2n-1)\cdot n(n+1)(n+2)\cdots(2(n-1))=2(2n-1)\cdot\mathrm{A}_{n-1}$. Επομένως $\mathrm{A}_n=2(2n-1)\cdot\mathrm{A}_{n-1}=2^2(2n-1)(2n-3)\mathrm{A}_{n-2}=\cdots=2^{n-1}(2n-1)(2n-3)\cdots5\cdot3\cdot\mathrm{A}_1=2^n\cdot1\cdot3\cdot5\cdots(2n-3)(2n-1)$, γιατί $\mathrm{A}_1=2$. Οι αριθμοί $1,3,5,\ldots,2n-3,2n-1$ είναι περιττοί και άρα και το γινόμενό τους περιττός. (Άσκηση 1.2. **(ii)**). ■

Άσκηση 15. Έστω $1\le\alpha_1<\alpha_2<\alpha_3<\cdots<\alpha_n<\alpha_{n+1}\le2n$, όπου n θετικός ακέραιος. Να δείξετε ότι υπάρχουν $i,j\in\{1,2,\ldots,n\}$ με $i\neq j$ τέτοιοι, ώστε $\alpha_i\mid\alpha_j$.

Απόδειξη: Έστω 2^{κ_i} η μεγαλύτερη δύναμη του 2 που διαιρεί τον α_i, για κάθε $i=1,2,\ldots,n+1$. Τότε $\kappa_i\ge0$ και $\alpha_i=2^{\kappa_i}\lambda_i$, όπου λ_i περιττός, για κάθε $i=1,\ldots,n+1$. Στο σύνολο $\{1,2,\ldots,2n\}$ υπάρχουν ακριβώς n περιττοί αριθμοί (και n άρτιοι). Εφόσον τα α_i είναι $n+1$ το πλήθος, θα υπάρχουν $i,j\in\{1,2,\ldots,n+1\}$ με $i<j$ και $\lambda_i=\lambda_j=\lambda$. Επειδή $\alpha_i<\alpha_j$, θα έχουμε $\kappa_i<\kappa_j$. Συνεπώς $\alpha_j=2^{\kappa_j}\lambda=2^{\kappa_j-\kappa_i}2^{\kappa_i}\lambda=2^{\kappa_j-\kappa_i}\alpha_i$, ήτοι $\alpha_i\mid\alpha_j$. ■

Στην προηγούμενη άσκηση εφαρμόσαμε τη λεγόμενη **αρχή του περιστερώνα**. Αυτή μας λέει απλά ότι αν έχουμε n αντικείμενα και τα τοποθετήσουμε σε k κουτιά, όπου $k<n$, τότε σίγουρα κάποιο κουτί θα έχει τουλάχιστον δύο στοιχεία. Εδώ οι αριθμοί α_i είναι $n+1$ το πλήθος και οι περιττοί λ_i είναι το πολύ $n<n+1$.

Άσκηση 16. Αν p,q είναι θετικοί ακέραιοι, τότε ο αριθμός $\left(p+\frac{1}{2}\right)^n+\left(q+\frac{1}{2}\right)^n$ είναι ακέραιος μόνο για πεπερασμένο πλήθος φυσικών αριθμών n.

Απόδειξη: Έχουμε: $\left(p+\frac{1}{2}\right)^n+\left(q+\frac{1}{2}\right)^n=\frac{(2p+1)^n+(2q+1)^n}{2^n}\in\mathbb{Z}\Leftrightarrow2^n\mid(2p+1)^n+(2q+1)^n$.

Οι αριθμοί $P=2p+1$ και $Q=2q+1$ είναι περιττοί. Θα αποδείξουμε ότι αν το n είναι περιττός, τότε η μεγαλύτερη δύναμη του 2 που διαιρεί το P^n+Q^n ισούται με τη μεγαλύτερη δύναμη του 2 που διαιρεί το $P+Q$, ενώ αν το $n\ge2$ είναι άρτιος, τότε η μεγαλύτερη δύναμη του 2 που διαιρεί το P^n+Q^n είναι το 2.

Πρώτα υποθέτουμε ότι το n είναι περιττός. Τότε $P^n+Q^n=(P+Q)(\underbrace{P^{n-1}-P^{n-2}Q+\cdots-PQ^{n-2}+Q^{n-1}}_{n\text{ περιττό πλήθος περιττών}})$.

Επομένως η παρένθεση είναι περιττός και επομένως η μεγαλύτερη δύναμη του 2 που διαιρεί το P^n+Q^n ισούται με τη μεγαλύτερη δύναμη του 2 που διαιρεί το $P+Q$.

Ας υποθέσουμε τώρα ότι το $n=2^\kappa$, όπου $\kappa\ge1$ είναι δύναμη του 2. Θα δείξουμε ότι η μεγαλύτερη δύναμη του 2 που διαιρεί το P^n+Q^n είναι το $2=2^1$. Προχωράμε επαγωγικά επί του κ.

Για $\kappa=1$ έχουμε: $P^2+Q^2=(P+Q)^2-2PQ\Leftrightarrow\frac{P^2+Q^2}{2}=\frac{(P+Q)^2}{2}-PQ$, με $2\Big|\frac{(P+Q)^2}{2}\Leftrightarrow4|(P+Q)^2$ και PQ περιττός. Άρα ο αριθμός $\frac{P^2+Q^2}{2}$ είναι περιττός ακέραιος και κατά συνέπεια η μεγαλύτερη δύναμη του 2 που διαιρεί το P^2+Q^2 είναι το $2=2^1$. Έστω τώρα ότι $1\le\kappa$ και ότι η μεγαλύτερη δύναμη του 2 που διαιρεί το $P^{2^\kappa}+Q^{2^\kappa}$ είναι το 2. Τότε, όπως προηγουμένως, $P^{2^{\kappa+1}}+Q^{2^{\kappa+1}}=(P^{2^\kappa}+Q^{2^\kappa})^2-2P^{2^\kappa}Q^{2^\kappa}\Leftrightarrow\frac{P^{2^{\kappa+1}}+Q^{2^{\kappa+1}}}{2}=\frac{(P^{2^\kappa}+Q^{2^\kappa})^2}{2}-P^{2^\kappa}Q^{2^\kappa}$ και από επαγωγή, η μεγαλύτερη δύναμη του 2 που διαιρεί το $\frac{(P^{2^\kappa}+Q^{2^\kappa})^2}{2}$ είναι το 2, ενώ το $P^{2^\kappa}Q^{2^\kappa}$ είναι περιττός. Άρα η μεγαλύτερη δύναμη του 2 που διαιρεί το $P^{2^{\kappa+1}}+Q^{2^{\kappa+1}}$ είναι το 2. Επαγωγικά λοιπόν έχουμε αποδείξει τον ισχυρισμό για δυνάμεις του 2.

Έστω τώρα $n=2^\kappa\lambda$ άρτιος ακέραιος, με $\kappa\ge1$ και $\lambda>1$ περιττός. Τότε $P^n+Q^n=P_1^\lambda+Q_1^\lambda$, όπου $P_1=P^{2^\kappa}$ και $Q_1=Q^{2^\kappa}$. Τότε, όπως στην πρώτη περίπτωση $P^n+Q^n=P_1^\lambda+Q_1^\lambda=(P_1+Q_1)(\underbrace{P_1^{\lambda-1}-P_1^{\lambda-2}Q_1+\cdots-P_1Q_1^{\lambda-2}+Q_1^{\lambda-1}}_{\lambda\text{ περιττό πλήθος περιττών}})$. Επομένως, η μεγαλύτερη δύναμη του 2 που διαιρεί το P^n+Q^n ισούται με τη μεγαλύτερη δύναμη του 2 που διαιρεί το $P_1+Q_1=P^{2^\kappa}+Q^{2^\kappa}$, η οποία με βάση τον προηγούμενο ισχυρισμό είναι το 2.

Το τελικό συμπέρασμα είναι ότι ο αριθμός $\left(p+\frac{1}{2}\right)^n+\left(q+\frac{1}{2}\right)^n$ είναι ακέραιος μόνον για $n=0$ ή $n=1$

ή n **περιττός** τέτοιος, ώστε το 2^n δεν υπερβαίνει τη μεγαλύτερη δύναμη του 2 η οποία διαιρεί τον αριθμό $P+Q=2(p+q+1)$, και σε καμία άλλη περίπτωση. (Αν $n\geq 2$ άρτιος, τότε $2^n>2^1$). ■

Άσκηση 17. Έστω α, β ακέραιοι. Υποθέτουμε ότι ο αριθμός $\alpha^2+2\beta$ είναι τέλειο τετράγωνο. Δείξτε ότι ο αριθμός $\alpha^2+\beta$ είναι άθροισμα δύο τετραγώνων.
Απόδειξη: Έστω $\alpha^2+2\beta=x^2$, για κάποιον ακέραιο x. Τότε $2\beta=x^2-\alpha^2$, άρτιος. Άρα οι α και x είναι και οι δύο άρτιοι ή και οι δύο περιττοί. Σε κάθε περίπτωση $2\mid x\pm\alpha\Leftrightarrow\dfrac{x\pm\alpha}{2}\in\mathbb{Z}$. Επίσης, $\beta=\dfrac{x^2-\alpha^2}{2}$.
Παρατηρούμε ότι: $\alpha^2+\beta=\alpha^2+\dfrac{x^2-\alpha^2}{2}=\dfrac{x^2+\alpha^2}{2}=\left(\dfrac{x+\alpha}{2}\right)^2+\left(\dfrac{x-\alpha}{2}\right)^2$. ■

ΑΛΥΤΕΣ ΑΣΚΗΣΕΙΣ

1. Μπορούμε να γράψουμε τον αριθμό 6^7 ως άθροισμα 1023 αριθμών, οι οποίοι να ανήκουν στο σύνολο $\{1,37,47,59\}$;

2. Έστω $\alpha,\beta,\gamma\in\mathbb{Z}$. Δείξτε ότι ο αριθμός $(\alpha+\beta)(\beta+\gamma)(\gamma+\alpha)$ είναι άρτιος.

3. Αν διαιρέσουμε το -313 με $\beta\neq 0$ παίρνουμε πηλίκο 35 και υπόλοιπο υ. Να βρεθούν οι β και υ.

4. Αν $\alpha\neq\beta$, να δείξετε ότι οι διαιρέσεις $\alpha:(\alpha-\beta)$ και $\beta:(\alpha-\beta)$ δίνουν το ίδιο υπόλοιπο.

5. Έστω $\alpha,\beta,\gamma\in\mathbb{Z}$ με $\beta\neq 0$. Η διαίρεση $\alpha:\beta$ δίνει πηλίκο 7 και υπόλοιπο 2. Η διαίρεση $\gamma:12$ δίνει πηλίκο α και υπόλοιπο 3β. Να βρεθούν οι α,β,γ.

6. Αν $n\geq 1$, δείξτε ότι $6\mid n(7n^2+5)$.

7. Αν $n\geq 1$, δείξτε τα επόμενα:
(i) $8\mid 5^{2n}+7$.
(ii) $15\mid 2^{4n}-1$.
(iii) $5\mid 3^{3n+1}+2^{n+1}$.
(iv) $21\mid 4^{n+1}+5^{2n-1}$.
(v) $24\mid 2\cdot 7^n+3\cdot 5^n-5$.

8. Αποδείξτε την ακόλουθη παραλλαγή της ευκλείδειας διαίρεσης: Αν $\alpha,\beta\in\mathbb{Z}$, με $\beta\neq 0$, υπάρχουν μοναδικοί ακέραιοι q, r τέτοιοι, ώστε $\alpha=q\beta+r$, με $-\frac{1}{2}|\beta|<r\leq\frac{1}{2}|\beta|$.

9. Δείξτε ότι αν για δύο ακεραίους α, β κάποιος από τους $2\alpha+3\beta$, $9\alpha+5\beta$ διαιρείται με το 17, τότε διαιρείται και ο άλλος.

10. Δείξτε τα ακόλουθα:
(i) Το άθροισμα των τετραγώνων δύο περιττών ακεραίων δεν είναι τέλειο τετράγωνο.
(ii) Το γινόμενο τεσσάρων διαδοχικών θετικών ακεραίων ισούται με το τετράγωνο ακεραίου, μειωμένο κατά 1.

11. Να δείξετε ότι για κάθε $n\in\mathbb{Z}$, ο αριθμός $8n+5$ δεν είναι τετράγωνο ακεραίου αριθμού.

12. Να βρείτε τους θετικούς ακεραίους n, ώστε ο αριθμός 2^n+5 να είναι τέλειο τετράγωνο.

13. **(i)** Να βρείτε τους θετικούς ακεραίους n, ώστε $n+2\mid n^2+2$.
(ii) Να βρείτε τους θετικούς ακεραίους n, ώστε $2n-1\mid n^2-n-1$.

14. Αν α είναι περιττός, τότε $12\mid\alpha^2+(\alpha+2)^2+(\alpha+4)^2+1$.

15. Να δείξετε ότι για κάθε θετικό ακέραιο n, ο αριθμός $1+7+7^2+\cdots+7^{4n-1}$ διαιρείται με το 400.

16. Να αποδείξετε τα παρακάτω:
(i) Για κάθε ακέραιο n, $6 \mid n(n^2+11)$.
(ii) Αν n είναι περιττός, τότε $24 \mid n(n^2-1)$.
(iii) Αν m και n είναι περιττοί, τότε $8 \mid m^2-n^2$.
(iv) Αν ο $m \in \mathbb{Z}$ δεν διαιρείται από το 2 και το 3, τότε $24 \mid m^2+23$.
(v) Αν m είναι ακέραιος, τότε $360 \mid m^2(m^2-1)(m^2-4)$.

17. Έστω $n>0$ άρτιος. Μπορούμε να γράψουμε το 1 στη μορφή $1=\frac{1}{k_1}+\frac{1}{k_2}+\cdots+\frac{1}{k_n}$, όπου $k_1,k_2,\ldots,k_n$ περιττοί;

18. Στην άσκηση 1.15 είδαμε ότι δεν μπορούμε να βρούμε ένα σύνολο $S \subseteq \{1,2,3,\ldots,2n\}$ από $n+1$ ακεραίους έτσι, ώστε $\alpha \nmid \beta$, για κάθε $\alpha,\beta \in S$, με $\alpha \neq \beta$. Ποιο είναι το μέγιστο πλήθος ενός συνόλου $S \subseteq \{1,2,3,\ldots,2n\}$ με την ιδιότητα $\alpha \nmid \beta$, για κάθε $\alpha,\beta \in S$, με $\alpha \neq \beta$;

1.2 Μέγιστος Κοινός Διαιρέτης και Ελάχιστο Κοινό Πολλαπλάσιο

Αν $\alpha \in \mathbb{Z}$, συμβολίζουμε με $\Delta(\alpha)$ το σύνολο των θετικών διαιρετών του α. Επειδή προφανώς $1 \in \Delta(\alpha)$, το σύνολο $\Delta(\alpha)$ δεν είναι κενό. Θεωρούμε τώρα δύο ακεραίους α και β, ένας τουλάχιστον εκ των οποίων δεν είναι μηδέν. Τότε το σύνολο $\Delta(\alpha)\cap\Delta(\beta)$ είναι άνω φραγμένο. Πράγματι, αν $\alpha \neq 0$, τότε από το **(ix)** της πρότασης 1.2, κάθε στοιχείο του $\Delta(\alpha)$ είναι μικρότερο ή ίσο του $|\alpha|$. Ομοίως, αν $\beta \neq 0$. Άρα το $\Delta(\alpha)$ ή το $\Delta(\beta)$ είναι άνω φραγμένο και το ίδιο προφανώς ισχύει για το υποσύνολό του $\Delta(\alpha)\cap\Delta(\beta)$. Επομένως το $\Delta(\alpha)\cap\Delta(\beta)$ περιέχει ένα μέγιστο στοιχείο.

Ορισμός 1.5. Το μέγιστο στοιχείο του $\Delta(\alpha)\cap\Delta(\beta)$ ονομάζεται **μέγιστος κοινός διαιρέτης των α και β** και συμβολίζεται με (α,β).

Από τον παραπάνω ορισμό και επειδή προφανώς $\Delta(\alpha)=\Delta(|\alpha|)$, θα έχουμε: $(\alpha,\beta)=(\beta,\alpha)$ και $(\alpha,\beta)=(|\alpha|,|\beta|)$.

Πρόταση 1.6. Αν $d=(\alpha,\beta)$, τότε το d είναι το ελάχιστο στοιχείο του συνόλου $A=\{\alpha x+\beta y \mid x,y \in \mathbb{Z} \text{ και } \alpha x+\beta y>0\}$.
Απόδειξη: Για $x=\alpha$ και $y=\beta$ έχουμε $\alpha x+\beta y=\alpha^2+\beta^2>0$, που σημαίνει ότι $\alpha^2+\beta^2 \in A$, ήτοι το A είναι μη κενό. Επειδή το A είναι προφανώς κάτω φραγμένο (από το 1), το A θα περιέχει (μοναδικό) ελάχιστο στοιχείο, το οποίο ας συμβολίσουμε με d. Έστω $d=\alpha x_0+\beta y_0$, $(x_0,y_0 \in \mathbb{Z})$.
Θα δείξουμε ότι το d είναι κοινός διαιρέτης των α και β. Έστω ότι $d \nmid \alpha$. Τότε $\alpha=d\pi+\upsilon$, με $\pi,\upsilon \in \mathbb{Z}$ και $0<\upsilon<d$. Τότε $\upsilon=\alpha-d\pi=\alpha-(\alpha x_0+\beta y_0)\pi=\alpha(1-x_0\pi)+\beta(-y_0\pi)$. Επομένως $\upsilon \in A$, άτοπο γιατί $0<\upsilon<d$ και το d είναι το ελάχιστο στοιχείο του A. Άρα $d \mid \alpha$ και παρόμοια $d \mid \beta$.
Έστω τώρα δ ένας κοινός θετικός διαιρέτης των α και β. Τότε $\delta \mid \alpha x_0+\beta y_0=d$ και συνεπώς $\delta \leq d$. Άρα ο d είναι ο μέγιστος κοινός διαιρέτης των α και β. ■

Πόρισμα 1.7. Κάθε κοινός διαιρέτης των α και β είναι διαιρέτης του (α,β).
Απόδειξη: Αν $d=(\alpha,\beta)$, τότε $d=\alpha x_0+\beta y_0$, για κάποια $x_0,y_0 \in \mathbb{Z}$, όπως προκύπτει από την απόδειξη της προηγούμενης πρότασης. Αν λοιπόν δ είναι ένας κοινός διαιρέτης των α και β, τότε $\delta \mid \alpha x_0+\beta y_0=d$. ■

Μπορούμε να ορίσουμε κατά τον ίδιο τρόπο τον μέγιστο κοινό διαιρέτη περισσοτέρων ακεραίων.

Ορισμός 1.8. Έστω $\alpha_1,\alpha_2,\ldots,\alpha_n \in \mathbb{Z}$, όπου $n=2,3,\ldots$ και κάποιος από τους α_i δεν είναι μηδέν. Τότε **ο μέγιστος κοινός διαιρέτης των $\alpha_1,\alpha_2,\ldots,\alpha_n$** ορίζεται ως το μέγιστο στοιχείο του $\Delta(\alpha_1)\cap\Delta(\alpha_2)\cap\cdots\cap\Delta(\alpha_n)$. Αυτός συμβολίζεται με $(\alpha_1,\alpha_2,\ldots,\alpha_n)$. (Υπάρχει μέγιστο στοιχείο γιατί, εφόσον $\alpha_i \neq 0$ για κάποιο $i=1,2,\ldots,n$, τότε κάθε κοινός (θετικός) διαιρέτης των $\alpha_1,\alpha_2,\ldots,\alpha_n$ δεν υπερβαίνει το $|\alpha_i|$).
Ανάλογα με την πρόταση 1.6 και το πόρισμα 1.7 έχουμε την ακόλουθη πρόταση, της οποίας η απόδειξη καίτοι είναι πανομοιότυπη με αυτήν των παραπάνω, αναφέρουμε χάριν πληρότητος.

Πρόταση 1.9. (i) Έστω $\mathrm{A}=\{\sum_{i=1}^{n} x_i\alpha_i \mid x_1,\ldots,x_n\in\mathbb{Z} \text{ και } \sum_{i=1}^{n} x_i\alpha_i>0\}$ το σύνολο των θετικών ακέραιων γραμμικών συνδυασμών των $\alpha_1,\alpha_2,\ldots,\alpha_n$. Τότε $(\alpha_1,\alpha_2,\ldots,\alpha_n)=\min \mathrm{A}$.
(ii) Κάθε κοινός διαιρέτης των $\alpha_1,\alpha_2,\ldots,\alpha_n$ διαιρεί τον $(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

Απόδειξη: Εφόσον κάποιος από τους $\alpha_1,\alpha_2,\ldots,\alpha_n$ δεν είναι μηδέν, έχουμε $0<\sum_{i=1}^{n}\alpha_i^2\in\mathrm{A}$ και άρα $\mathrm{A}\neq\varnothing$. Έστω $d=\min \mathrm{A}$. Τότε $d=\sum_{i=1}^{n} x_i\alpha_i$, για κάποιους $x_1,\ldots,x_n\in\mathbb{Z}$. Θα δείξουμε τώρα ότι $d\mid\alpha_j$, για κάθε $j=1,2,\ldots,n$. Έστω ότι $d\nmid\alpha_j$, για κάποιο $j\in\{1,2,\ldots,n\}$. Τότε $\alpha_j=d\pi+\upsilon$, όπου $\pi,\upsilon\in\mathbb{Z}$ και $0<\upsilon<d$. Τότε $\upsilon=\alpha_j-\pi d=\alpha_j-\sum_{i=1}^{n}\pi x_i\alpha_i=\sum_{i=1}^{n} y_i\alpha_i$, όπου $y_i=-\pi x_i$ αν $i\neq j$ και $y_j=1-\pi x_j$. Επομένως $\upsilon\in\mathrm{A}$, άτοπο γιατί $d=\min \mathrm{A}$. Κατά συνέπεια το d διαιρεί καθέναν από τους $\alpha_1,\alpha_2,\ldots,\alpha_n$.
Τώρα, το d είναι ο μέγιστος κοινός διαιρέτης των $\alpha_1,\alpha_2,\ldots,\alpha_n$ και μάλιστα αν δ είναι ένας θετικός κοινός διαιρέτης αυτών, τότε $\delta\mid d$ (και κατά συνέπεια $\delta\leq d$). Έστω λοιπόν $\delta\in\Delta(\alpha_1)\cap\Delta(\alpha_2)\cap\cdots\cap\Delta(\alpha_n)$. Τότε $\delta\mid\alpha_i$, για κάθε $i=1,2,\ldots,n$ και επομένως $\delta\mid\sum_{i=1}^{n} x_i\alpha_i=d$. ■

Πρόταση 1.10. Έστω $n\geq 3$ και $1<k<n$, όπου k,n θετικοί ακέραιοι. Τότε ισχύει η σχέση:

$$(\alpha_1,\alpha_2,\ldots,\alpha_n)=((\alpha_1,\alpha_2,\ldots,\alpha_k),(\alpha_{k+1},\alpha_{k+2},\ldots,\alpha_n)).$$

Απόδειξη: Έστω $d=(\alpha_1,\alpha_2,\ldots,\alpha_n)$ και $d'=((\alpha_1,\alpha_2,\ldots,\alpha_k),(\alpha_{k+1},\alpha_{k+2},\ldots,\alpha_n))$. Επίσης θέτουμε $d_1=(\alpha_1,\alpha_2,\ldots,\alpha_k)$ και $d_2=(\alpha_{k+1},\alpha_{k+2},\ldots,\alpha_n)$. Τότε $d\mid\alpha_i$, για κάθε $i=1,\ldots,k$ και επομένως $d\mid(\alpha_1,\alpha_2,\ldots,\alpha_k)=d_1$. Επίσης, $d\mid\alpha_i$, για κάθε $i=k+1,\ldots,n$ και επομένως $d\mid(\alpha_{k+1},\ldots,\alpha_n)=d_2$. Κατά συνέπεια $d\mid(d_1,d_2)=d'$. Αντιστρόφως, $d'=(d_1,d_2)\mid d_1$ και $d_1\mid\alpha_i$, για κάθε $i=1,\ldots,k$. Άρα $d'\mid\alpha_i$, για κάθε $i=1,\ldots,k$. Ακόμη, $d'=(d_1,d_2)\mid d_2$ και $d_2\mid\alpha_i$, για κάθε $i=k+1,\ldots,n$. Συμπεραίνουμε ότι $d'\mid\alpha_i$, για κάθε $i=1,2,\ldots,n$ και επομένως $d'\mid(\alpha_1,\alpha_2,\ldots,\alpha_n)=d$. Αφού $d\mid d'$ και $d'\mid d$, προκύπτει ότι $d=d'$. ■

Πρόταση 1.11. Αν $\mu,\lambda\in\mathbb{Z}$, τότε $(\alpha,\beta)=(\alpha+\lambda\beta,\beta)=(\alpha,\beta+\mu\alpha)$.
Απόδειξη: Έστω $d_1=(\alpha,\beta)$ και $d_2=(\alpha+\lambda\beta,\beta)$. Τότε $d_1\mid\alpha$ και $d_1\mid\beta\Rightarrow d_1\mid\lambda\beta$. Άρα $d_1\mid\alpha+\lambda\beta$ και συνεπώς $d_1\mid(\alpha+\lambda\beta,\beta)=d_2$. Αντιστρόφως, $d_2\mid\beta\Rightarrow d_2\mid\lambda\beta$ και επειδή $d_2\mid\alpha+\lambda\beta$, $d_2\mid\alpha+\lambda\beta-\lambda\beta=\alpha$. Άρα $d_2\mid\alpha$ και $d_2\mid\beta$ και επομένως $d_2\mid(\alpha,\beta)=d_1$. Ομοίως αποδεικνύεται ότι $(\alpha,\beta)=(\alpha,\beta+\mu\alpha)$. ■

Επομένως, $(\alpha,\beta)=(\alpha-2\beta,\beta)=(\alpha,3\alpha+\beta)$ κτλ.

Πόρισμα 1.12. Έστω $\alpha,\beta\in\mathbb{Z}$ με $\beta\neq 0$. Αν $\alpha=\beta\pi+\upsilon$ είναι η ταυτότητα της ευκλείδειας διαίρεσης $\alpha:\beta$, τότε $(\alpha,\beta)=(\beta,\upsilon)$.
Απόδειξη: $(\alpha,\beta)=(\alpha-\pi\beta,\beta)=(\upsilon,\beta)=(\beta,\upsilon)$. ■

Το παραπάνω πόρισμα μας επιτρέπει να βρίσκουμε τον μέγιστο κοινό διαιρέτη δύο ακεραίων. Κατ' αρχάς, επειδή $(\alpha,\beta)=(|\alpha|,|\beta|)$, μπορούμε να υποθέσουμε ότι οι ακέραιοι είναι μη αρνητικοί και βεβαίως ένας τουλάχιστον π.χ. ο β θετικός.
Διαιρούμε τον α με τον β και παίρνουμε πηλίκο π και υπόλοιπο υ. Τότε $(\alpha,\beta)=(\beta,\upsilon)$, με $0\leq\upsilon<\beta$. Αν $\upsilon=0$, τότε $(\alpha,\beta)=\beta$. Αν όχι, τότε διαιρούμε το β με το υ και παίρνουμε πηλίκο π_1 και υπόλοιπο υ_1, με $0\leq\upsilon_1<\upsilon$. Αν $\upsilon_1=0$, τότε $(\alpha,\beta)=(\beta,\upsilon)=(\upsilon,\upsilon_1)=\upsilon$. Αν όχι, τότε διαιρούμε το υ με το υ_1 και παίρνουμε πηλίκο π_2 και υπόλοιπο υ_2. Τότε $(\alpha,\beta)=(\beta,\upsilon)=(\upsilon,\upsilon_1)=(\upsilon_1,\upsilon_2)$ κ.ο.κ. Επειδή $\beta>\upsilon>\upsilon_1>\upsilon_2>\cdots\geq 0$, η διαδικασία αυτή κάποτε θα σταματήσει. Έχουμε λοιπόν τις σχέσεις:

$$\left.\begin{array}{ll}
\alpha=\beta\pi+\upsilon & (\mathrm{A}_1)\\
\beta=\upsilon\pi_1+\upsilon_1 & (\mathrm{A}_2)\\
\upsilon=\upsilon_1\pi_2+\upsilon_2 & (\mathrm{A}_3)\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
\upsilon_{n-3}=\upsilon_{n-2}\pi_{n-1}+\upsilon_{n-1} & (\mathrm{A}_n)\\
\upsilon_{n-2}=\upsilon_{n-1}\pi_n+\boxed{\upsilon_n} & (\mathrm{A}_{n+1})\\
\upsilon_{n-1}=\upsilon_n\pi_{n+1} & (\mathrm{A}_{n+2})
\end{array}\right\},$$

όπου έχουμε θεωρήσει $\upsilon_{n+1} = 0$. Επομένως, $(\alpha, \beta) = (\beta, \upsilon) = (\upsilon, \upsilon_1) = (\upsilon_1, \upsilon_2) = \cdots = (\upsilon_{n-2}, \upsilon_{n-1}) = (\upsilon_{n-1}, \upsilon_n) = (\upsilon_n, 0) = \upsilon_n$. Η παραπάνω μέθοδος λέγεται **Ευκλείδειος Αλγόριθμος**.

Παράδειγμα 1.13. Να βρεθεί ο $(-1155, 180)$. Στη συνέχεια να γραφεί ο $(-1155, 180)$ ως ακέραιος γραμμικός συνδυασμός των -1155 και 180.
Λύση: Επειδή $(\alpha, \beta) = (|\alpha|, |\beta|)$, αρκεί να υπολογίσουμε τον $(1155, 180)$. Εφαρμόζουμε τον αλγόριθμο του Ευκλείδη:

$$\left.\begin{array}{ll} 1155 = 180 \cdot 6 + 75 & (\mathrm{A}_1) \\ 180 = 75 \cdot 2 + 30 & (\mathrm{A}_2) \\ 75 = 30 \cdot 2 + \boxed{15} & (\mathrm{A}_3) \\ 30 = 15 \cdot 2 & (\mathrm{A}_4) \end{array}\right\},$$

Επομένως $(-1155, 180) = (1155, 180) = 15$.
Οι σχέσεις (A_1), (A_2) και (A_3) γράφονται ισοδύναμα στη μορφή:

$$\left.\begin{array}{ll} 75 = 1155 - 6 \cdot 180\cdot & (\mathrm{A}'_1) \\ 30 = 180 - 2 \cdot 75 & (\mathrm{A}'_2) \\ 15 = 75 - 2 \cdot 30 & (\mathrm{A}'_3) \end{array}\right\},$$

Επομένως, $15 = 75 - 2 \cdot 30 = 75 - 2 \cdot (180 - 2 \cdot 75) = -2 \cdot 180 + 5 \cdot 75 = -2 \cdot 180 + 5 \cdot (1155 - 6 \cdot 180) = 5 \cdot 1155 - 32 \cdot 180$. Άρα $15 = (-5) \cdot (-1155) + (-32) \cdot 180$, ο ζητούμενος γραμμικός συνδυασμός. ■

Παρατηρήστε ότι δεν κάναμε πράξεις μεταξύ των εμπλεκομένων πηλίκων και υπολοίπων, αλλά μόνο με τους συντελεστές αυτών. Η διαδικασία αυτή γενικεύεται. Οι σχέσεις (A_1), (A_2) $, \ldots, (\mathrm{A}_{n+1})$ ισοδυναμούν με τις σχέσεις

$$\left.\begin{array}{ll} \upsilon = \alpha - \pi\beta & (\mathrm{A}'_1) \\ \upsilon_1 = \beta - \pi_1\upsilon & (\mathrm{A}'_2) \\ \upsilon_2 = \upsilon - \pi_2\upsilon_1 & (\mathrm{A}'_3) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ \upsilon_{n-1} = \upsilon_{n-3} - \pi_{n-1}\upsilon_{n-2} & (\mathrm{A}'_n) \\ \upsilon_n = \upsilon_{n-2} - \pi_n\upsilon_{n-1} & (\mathrm{A}'_{n+1}) \end{array}\right\}$$

Μπορούμε λοιπόν να γράψουμε το υ_n ως γραμμικό συνδυασμό των υ_{n-1} και υ_{n-2}, στη συνέχεια να αντικαταστήσουμε το υ_{n-1} με γραμμικό συνδυασμό των υ_{n-2} και υ_{n-3} κ.ο.κ., μέχρι να καταλήξουμε σ' έναν γραμμικό συνδυασμό των α και β. Επειδή $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n) = ((\alpha_1, \alpha_2, \ldots, \alpha_{n-1}), \alpha_n)$, η διαδικασία αυτή επεκτείνεται επαγωγικά. Αν γράψουμε τον $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$ ως γραμμικό συνδυασμό των $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ και στη συνέχεια γράψουμε τον $((\alpha_1, \alpha_2, \ldots, \alpha_{n-1}), \alpha_n)$ ως γραμμικό συνδυασμό των $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$ και α_n, τότε θα πάρουμε έναν γραμμικό συνδυασμό των $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n$, ο οποίος θα ισούται με τον $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n)$.

Παράδειγμα 1.14. Να εκφράσετε τον $(315, 390, 102)$ ως γραμμικό συνδυασμό των $315, 390$ και 102.
Λύση: Έχουμε τις σχέσεις: $390 = 315 + 75$, $315 = 4 \cdot 75 + 15$, $75 = 5 \cdot 15$. Επομένως. $(315, 390) = 15$ και $15 = 315 - 4 \cdot 75 = 315 - 4 \cdot (390 - 315) = 5 \cdot 315 + (-4) \cdot 390$.
Στη συνέχεια εκφράζουμε τον $(15, 102)$ ως γραμμικό συνδυασμό των 15 και 102. Έχουμε: $102 = 6 \cdot 15 + 12$, $15 = 12 + 3$ και $12 = 4 \cdot 3$. Άρα $(315, 390, 102) = (15, 102) = 3$. Επίσης, $3 = 15 - 12 = 15 - (102 - 6 \cdot 15) = 7 \cdot 15 + (-1) \cdot 102$ και επομένως
$3 = 7 \cdot \big(5 \cdot 315 + (-4) \cdot 390\big) + (-1) \cdot 102 = 35 \cdot 315 + (-28) \cdot 390 + (-1) \cdot 102$. ■

Ορισμός 1.15. Δύο ακέραιοι α, β λέγονται **σχετικώς πρώτοι** ή **πρώτοι μεταξύ τους** αν $(\alpha, \beta) = 1$.

Πόρισμα 1.16. (Ευκλείδης) Έστω $\alpha_1 \mid \alpha$ και $\beta_1 \mid \beta$. Τότε $(\alpha_1, \beta_1) \mid (\alpha, \beta)$. Ιδιαιτέρως αν $(\alpha, \beta) = 1$, τότε $(\alpha_1, \beta_1) = 1$.
Απόδειξη: Έστω $\delta = (\alpha, \beta)$ και $\delta_1 = (\alpha_1, \beta_1)$. Έχουμε $\delta_1 \mid \alpha_1$ και $\alpha_1 \mid \alpha$. Άρα $\delta_1 \mid \alpha$. Ομοίως $\delta_1 \mid \beta$. Άρα $\delta_1 \mid (\alpha, \beta) = \delta$. ■

Με απλά λόγια το προηγούμενο πόρισμα, στην περίπτωση που $(\alpha,\beta)=1$, μας λέει ότι και κάθε διαιρέτης του α θα είναι πρώτος προς τον β, αλλά και κάθε διαιρέτη του β. Ομοίως κάθε διαιρέτης του β θα είναι πρώτος προς τον α, αλλά και κάθε διαιρέτη του α. Το προηγούμενο πόρισμα γενικεύεται εύκολα:

Άσκηση 18. Έστω $\alpha_i \mid \beta_i$, για κάθε $i=1,2,\ldots,n$, όπου $n\geq 2$. Δείξτε ότι $(\alpha_1,\alpha_2,\ldots,\alpha_n)\mid(\beta_1,\beta_2,\ldots,\beta_n)$.
Απόδειξη: Για $n=2$ είναι το προηγούμενο πόρισμα. Έστω $n>2$ και υποθέτουμε ότι ο ισχυρισμός ισχύει για $n-1$. Αν λοιπόν $\alpha_i\mid\beta_i$, για κάθε $i=1,2,\ldots,n$, τότε θα έχουμε $(\alpha_1,\alpha_2,\ldots,\alpha_{n-1})\mid(\beta_1,\beta_2,\ldots,\beta_{n-1})$. Αλλά και $\alpha_n\mid\beta_n$. Από το προηγούμενο πόρισμα (για $n=2$) προκύπτει ότι $(\alpha_1,\alpha_2,\ldots,\alpha_{n-1},\alpha_n)=$ $=((\alpha_1,\alpha_2,\ldots,\alpha_{n-1}),\alpha_n)\mid((\beta_1,\beta_2,\ldots,\beta_{n-1}),\beta_n)=(\beta_1,\beta_2,\ldots,\beta_{n-1},\beta_n)$. ■

Λήμμα 1.17. (Λήμμα του Ευκλείδη) Έστω $\alpha\mid\beta\gamma$ και $(\alpha,\beta)=1$. Τότε $\alpha\mid\gamma$.
Απόδειξη: Έχουμε $1=(\alpha,\beta)=\alpha x+\beta y$, για κάποιους $x,y\in\mathbb{Z}$. Επομένως $\gamma=\alpha\gamma x+\beta\gamma y$. Προφανώς $\alpha\mid\alpha\gamma x$ και $\alpha\mid(\beta\gamma)y$. Συνεπώς $\alpha\mid\alpha\gamma x+\beta\gamma y=\gamma$. ■

Ως συμπέρασμα προκύπτει το ακόλουθο **σημαντικό λήμμα**:

Λήμμα 1.18. (Ευκλείδης) Αν $(\alpha,\beta)=1$, τότε $(\alpha,\beta\gamma)=(\alpha,\gamma)$.
Απόδειξη: Έστω $\delta=(\alpha,\beta\gamma)$ και $\delta'=(\alpha,\gamma)$. Έχουμε $\delta'\mid\gamma\Rightarrow\delta'\mid\beta\gamma$. Επειδή δε $\delta'\mid\alpha$, έπεται ότι $\delta'\mid(\alpha,\beta\gamma)=\delta$. Αντιστρόφως, $\delta\mid\alpha$ και $\beta\mid\beta$. Από το πόρισμα 1.16 προκύπτει ότι $(\delta,\beta)=1$. Αλλά $\delta\mid\beta\gamma$. Από το Λήμμα του Ευκλείδη προκύπτει ότι $\delta\mid\gamma$. Εφόσον λοιπόν $\delta\mid\alpha$ και $\delta\mid\gamma$, θα έχουμε $\delta\mid(\alpha,\gamma)=\delta'$. ■

Άσκηση 19. Έστω $\alpha>1$ και m,n θετικοί ακέραιοι.
(i) Αν $m\mid n$, να δείξετε ότι $\alpha^m-1\mid\alpha^n-1$.
(ii) Γενικά ισχύει η σχέση: $(\alpha^m-1,\alpha^n-1)=\alpha^{(m,n)}-1$.
(iii) Γενικά ισχύει η ισοδυναμία: $\alpha^m-1\mid\alpha^n-1\Leftrightarrow m\mid n$.
Απόδειξη: (i) Έστω $n=\lambda m$. Τότε $\alpha^n-1=(\alpha^m)^\lambda-1=(\alpha^m-1)(\alpha^{m(\lambda-1)}+\alpha^{m(\lambda-2)}+\cdots+1)$.
(ii) Έστω $d=(m,n)$. Εφαρμόζουμε τον ευκλείδειο αλγόριθμο για προσδιορίσουμε τον d.

$$\left.\begin{array}{ll} n=m\pi+\upsilon & (\mathrm{A}_1)\\ m=\upsilon\pi_1+\upsilon_1 & (\mathrm{A}_2)\\ \upsilon=\upsilon_1\pi_2+\upsilon_2 & (\mathrm{A}_3)\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ \upsilon_{t-3}=\upsilon_{t-2}\pi_{t-1}+\upsilon_{t-1} & (\mathrm{A}_t)\\ \upsilon_{t-2}=\upsilon_{t-1}\pi_t+\boxed{d} & (\mathrm{A}_{t+1})\\ \upsilon_{t-1}=d\pi_{t+1} & (\mathrm{A}_{t+2}) \end{array}\right\}$$

Από το **(i)** προκύπτει ότι το $\alpha^{m\pi}-1$ είναι πολλαπλάσιο του α^m-1. Επομένως $(\alpha^m-1,\alpha^n-1)=$ $=(\alpha^m-1,\alpha^{m\pi+\upsilon}-1)=(\alpha^m-1,\alpha^{m\pi+\upsilon}-\alpha^{m\pi}+\alpha^{m\pi}-1)$. Επειδή $\alpha^m-1\mid\alpha^{m\pi}-1$, από την πρόταση 1.11 προκύπτει ότι το τελευταίο ισούται με $(\alpha^m-1,\alpha^{m\pi+\upsilon}-\alpha^{m\pi})=(\alpha^m-1,\alpha^{m\pi}(\alpha^\upsilon-1))$. Παρατηρούμε ότι $(\alpha^m-1,\alpha^{m\pi})=1$. Πράγματι, αν $\delta=(\alpha^m-1,\alpha^{m\pi})$, τότε $\delta\mid\alpha^m-1$ και $\alpha^m-1\mid\alpha^{m\pi}-1$. Άρα $\delta\mid\alpha^{m\pi}-1$ και επειδή $\delta\mid\alpha^{m\pi}$, έπεται ότι $\delta\mid\alpha^{m\pi}-(\alpha^{m\pi-1})=1$. Από το λήμμα 1.18 παίρνουμε $(\alpha^m-1,\alpha^{m\pi}(\alpha^\upsilon-1))=(\alpha^m-1,\alpha^\upsilon-1)$.
Στη συνέχεια διαιρούμε το m με το υ και παίρνουμε $(\alpha^\upsilon-1,\alpha^m-1)=(\alpha^\upsilon-1,\alpha^{\upsilon_1}-1)$. Προχωρώντας κατ' αυτόν τον τρόπο έχουμε: $(\alpha^m-1,\alpha^n-1)=(\alpha^m-1,\alpha^\upsilon-1)=(\alpha^\upsilon-1,\alpha^{\upsilon_1}-1)=\cdots=(\alpha^{\upsilon_{t-1}}-1,\alpha^{\upsilon_t}-1)=$ $=(\alpha^{\upsilon_{t-1}}-1,\alpha^d-1)=\alpha^d-1$, γιατί $d\mid\upsilon_{t-1}$.
(iii) $\alpha^m-1\mid\alpha^n-1\Leftrightarrow(\alpha^m-1,\alpha^n-1)=\alpha^m-1\underset{\textbf{(ii)}}{\Leftrightarrow}\alpha^{(m,n)}-1=\alpha^m-1\Leftrightarrow(m,n)=m\Leftrightarrow m\mid n$. ■

Λήμμα 1.19. Έστω $\alpha_1,\alpha_2,\ldots,\alpha_n\in\mathbb{Z}$, όχι όλοι μηδέν. Έστω επίσης $\lambda\in\mathbb{Z}\setminus\{0\}$. Τότε $(\lambda\alpha_1,\lambda\alpha_2,\ldots,\lambda\alpha_n)$ $=|\lambda|(\alpha_1,\alpha_2,\ldots,\alpha_n)$.
Απόδειξη: Υποθέτουμε πρώτα ότι $\lambda>0$. Εφόσον $\lambda\mid\lambda\alpha_1$, $\lambda\mid\lambda\alpha_2,\ldots$, $\lambda\mid\lambda\alpha_n$, τότε το λ θα

διαιρεί τον $(\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_n)$. Έστω $\delta = \dfrac{(\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_n)}{\lambda}$, θετικός ακέραιος. Επομένως $\lambda\delta = (\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_n)$. Άρα $\lambda\delta \mid \lambda\alpha_i$, για κάθε $i = 1, \ldots, n$. Επομένως $\delta \mid \alpha_i$, για κάθε $i = 1, \ldots, n$ και κατά συνέπεια, $\delta \mid (\alpha_1, \alpha_2, \ldots, \alpha_n) =: \delta'$. Αλλά $\delta' \mid \alpha_i$, για κάθε $i = 1, \ldots, n$ και συνεπώς $\lambda\delta' \mid \lambda\alpha_i$, για κάθε $i = 1, \ldots, n$. Επομένως $\lambda\delta' \mid (\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_n) = \lambda\delta \Rightarrow \delta' \mid \delta$. Άρα $\delta = \delta' = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Συμπεραίνουμε λοιπόν ότι $(\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_n) = \lambda(\alpha_1, \alpha_2, \ldots, \alpha_n)$.
Αν τώρα $\lambda < 0$, τότε $(\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_n) = (|\lambda\alpha_1|, |\lambda\alpha_2|, \ldots, |\lambda\alpha_n|) = |\lambda|(|\alpha_1|, |\alpha_2|, \ldots, |\alpha_n|) = |\lambda|(\alpha_1, \alpha_2, \ldots, \alpha_n)$. ■

Πόρισμα 1.20. Αν $0 < \delta \mid \alpha_i$, για κάθε $i = 1, 2, \ldots, n$ $\big($ισοδύναμα $\delta \mid (\alpha_1, \alpha_2 \ldots, \alpha_n)\big)$, τότε

$$\frac{(\alpha_1, \alpha_2, \ldots, \alpha_n)}{\delta} = \Big(\frac{\alpha_1}{\delta}, \frac{\alpha_2}{\delta}, \ldots, \frac{\alpha_n}{\delta}\Big).$$

Ιδιαιτέρως, αν $\delta = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, τότε $\Big(\dfrac{\alpha_1}{\delta}, \dfrac{\alpha_2}{\delta}, \ldots, \dfrac{\alpha_n}{\delta}\Big) = 1$.

Απόδειξη: $\delta \cdot \Big(\dfrac{\alpha_1}{\delta}, \dfrac{\alpha_2}{\delta}, \ldots, \dfrac{\alpha_n}{\delta}\Big) = \Big(\delta \cdot \dfrac{\alpha_1}{\delta}, \delta \cdot \dfrac{\alpha_2}{\delta}, \ldots, \delta \cdot \dfrac{\alpha_n}{\delta}\Big) = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. ■

Ως εφαρμογή των παραπάνω έχουμε την ακόλουθη πρόταση:

Πρόταση 1.21. (i) $(\alpha, \beta_1\beta_2 \cdots \beta_n) \mid (\alpha, \beta_1)(\alpha, \beta_2) \cdots (\alpha, \beta_n)$.
(ii) Υποθέτουμε ότι $(\alpha, \beta_i) = 1$, για κάθε $i = 1, 2, \ldots, n$. Τότε $(\alpha, \beta_1\beta_2 \cdots \beta_n) = 1$.
(iii) (Ευκλείδης) Έστω $\alpha_i \mid \beta$, για κάθε $i = 1, 2, \ldots, n$. Έστω επίσης ότι $(\alpha_i, \alpha_j) = 1$, για κάθε i, j με $i \neq j$. Τότε $\alpha_1\alpha_2 \cdots \alpha_n \mid \beta$.
(iv) Αν $(\beta_i, \beta_j) = 1$ για κάθε $i, j \in \{1, 2, \ldots, n\}$ με $i \neq j$, τότε $(\alpha, \beta_1\beta_2 \cdots \beta_n) = (\alpha, \beta_1)(\alpha, \beta_2) \cdots (\alpha, \beta_n)$.
Απόδειξη: (i) Εφαρμόζουμε επαγωγή επί του n. Για $n = 1$ δεν έχουμε τίποτα να αποδείξουμε. Έστω $n = 2$. Θέτουμε $\delta = (\alpha, \beta_1\beta_2)$. Επειδή $(\alpha, \beta_1) \mid \alpha$ και $(\alpha, \beta_1) \mid \beta_1$ (άρα και $(\alpha, \beta_1) \mid \beta_1\beta_2$), παίρνουμε $(\alpha, \beta_1) \mid (\alpha, \beta_1\beta_2) = \delta$. Τώρα, $\dfrac{\delta}{(\alpha, \beta_1)} = \Big(\dfrac{\alpha}{(\alpha, \beta_1)}, \dfrac{\beta_1}{(\alpha, \beta_1)}\beta_2\Big)$. Αλλά $\Big(\dfrac{\alpha}{(\alpha, \beta_1)}, \dfrac{\beta_1}{(\alpha, \beta_1)}\Big) = 1$. Σύμφωνα με το λήμμα 1.18, $\dfrac{\delta}{(\alpha, \beta_1)} = \Big(\dfrac{\alpha}{(\alpha, \beta_1)}, \beta_2\Big)$. Αλλά $\Big(\dfrac{\alpha}{(\alpha, \beta_1)}, \beta_2\Big) \mid (\alpha, \beta_2)$, βάσει του πορίσματος 1.16, επειδή $\dfrac{\alpha}{(\alpha, \beta_1)} \mid \alpha$. Συνεπώς $\delta \mid (\alpha, \beta_1)(\alpha, \beta_2)$.
Επαγωγικά, αν $n > 2$, υποθέτουμε ότι $(\alpha, \beta_1\beta_2 \cdots \beta_{n-1}) \mid (\alpha, \beta_1)(\alpha, \beta_2) \cdots (\alpha, \beta_{n-1})$.
Τότε $(\alpha, \beta_1\beta_2 \cdots \beta_{n-1}\beta_n) = (\alpha, (\beta_1\beta_2 \cdots \beta_{n-1})\beta_n) \mid (\alpha, \beta_1\beta_2 \cdots \beta_{n-1})(\alpha, \beta_n)$ και επειδή $(\alpha, \beta_1\beta_2 \cdots \beta_{n-1}) \mid (\alpha, \beta_1)(\alpha, \beta_2) \cdots (\alpha, \beta_{n-1})$, έπεται ότι $(\alpha, \beta_1\beta_2 \cdots \beta_{n-1}\beta_n) \mid (\alpha, \beta_1)(\alpha, \beta_2) \cdots (\alpha, \beta_{n-1})(\alpha, \beta_n)$.
(ii) Αυτό προκύπτει από το **(i)**, αφού $(\alpha, \beta_1\beta_2 \cdots \beta_n) \mid (\alpha, \beta_1)(\alpha, \beta_2) \cdots (\alpha, \beta_n) = 1$.
(iii) Έστω $n = 2$. Υποθέτουμε ότι $\alpha_1 \mid \beta$, $\alpha_2 \mid \beta$ και $(\alpha_1, \alpha_2) = 1$. Εφόσον $\alpha_1 \mid \beta$, το β γράφεται $\beta = \lambda\alpha_1$. Αλλά $\alpha_2 \mid \beta = \lambda\alpha_1$ και $(\alpha_1, \alpha_2) = 1$. Από το λήμμα του Ευκλείδη προκύπτει ότι $\alpha_2 \mid \lambda$ και άρα $\lambda = \lambda'\alpha_2$. Άρα $\beta = \lambda'\alpha_1\alpha_2 \Rightarrow \alpha_1\alpha_2 \mid \beta$. Επαγωγικά υποθέτουμε ότι $n > 2$ και ότι ο ισχυρισμός ισχύει για $n - 1$. Θα αποδείξουμε ότι ισχύει και για n. Έστω λοιπόν $\alpha_i \mid \beta$, για κάθε $i = 1, 2, \ldots, n$ και ότι $(\alpha_i, \alpha_j) = 1$, για κάθε i, j με $i \neq j$. Τότε $\alpha_1\alpha_2 \cdots \alpha_{n-1} \mid \beta$. Σύμφωνα με το **(ii)** $(\alpha_1\alpha_2 \cdots \alpha_{n-1}, \alpha_n) = 1$. Εφόσον λοιπόν $\alpha_1\alpha_2 \cdots \alpha_{n-1} \mid \beta$ και $\alpha_n \mid \beta$, θα έχουμε (εδώ εφαρμόζουμε την περίπτωση $n = 2$ που αποδείξαμε) ότι $\alpha_1\alpha_2 \cdots \alpha_{n-1}\alpha_n \mid \beta$.
(iv) Από το **(i)** έχουμε $(\alpha, \beta_1\beta_2 \cdots \beta_n) \mid (\alpha, \beta_1)(\alpha, \beta_2) \cdots (\alpha, \beta_n)$. Παρατηρούμε ότι $((\alpha, \beta_i), (\alpha, \beta_j)) = 1$, για $i \neq j$ γιατί $(\alpha, \beta_i) \mid \beta_i$, $(\alpha, \beta_j) \mid \beta_j$ και $(\beta_i, \beta_j) = 1$ και κατά συνέπεια, βάσει του πορίσματος 1.16, οι αριθμοί (α, β_i) (α, β_j) είναι πρώτοι μεταξύ τους. Επειδή $(\alpha, \beta_i) \mid (\alpha, \beta_1\beta_2 \cdots \beta_n)$, για κάθε $i = 1, 2, \ldots, n$, από το **(iii)** προκύπτει ότι $(\alpha, \beta_1)(\alpha, \beta_2) \cdots (\alpha, \beta_n) \mid (\alpha, \beta_1\beta_2 \cdots \beta_n)$. ■

Πόρισμα 1.22. (i) Αν m, n είναι θετικοί ακέραιοι, δείξτε την ισοδυναμία: $(\alpha, \beta) = 1 \Leftrightarrow (\alpha^m, \beta^n) = 1$.
(ii) $(\alpha_1^k, \alpha_2^k, \ldots, \alpha_n^k) = (\alpha_1, \alpha_2, \ldots, \alpha_n)^k$, για κάθε θετικό ακέραιο k.
Απόδειξη: (i) Η συνεπαγωγή $(\alpha, \beta) = 1 \Rightarrow (\alpha, \beta^n) = 1$ προκύπτει από το **(ii)** της προηγούμενης πρότασης, αν θέσουμε $\beta_1 = \beta_2 = \cdots = \beta_n = \beta$. Ομοίως, $(\beta^n, \alpha) = 1 \Rightarrow (\beta^n, \alpha^m) = 1$. Τελικά, $(\alpha, \beta) = 1 \Rightarrow (\alpha^m, \beta^n) = 1$. Το αντίστροφο προκύπτει από το πόρισμα 1.16, αφού $\alpha \mid \alpha^m$ και $\beta \mid \beta^n$.

(ii) Έστω $n = 2$ και $\delta = (\alpha_1, \alpha_2) \Leftrightarrow \left(\frac{\alpha_1}{\delta}, \frac{\alpha_2}{\delta}\right) = 1$. Τότε από το **(i)**, για $m = n = k$ προκύπτει ότι $\left(\frac{\alpha_1^k}{\delta^k}, \frac{\alpha_2^k}{\delta^k}\right) = 1$. Άρα $(\alpha_1^k, \alpha_2^k) = \delta^k = (\alpha_1, \alpha_2)^k$. Αν $n > 2$, επαγωγικά έχουμε: $(\alpha_1^k, \alpha_2^k, \ldots, \alpha_{n-1}^k, \alpha_n^k) = (((\alpha_1^k, \alpha_2^k, \ldots, \alpha_{n-1}^k), \alpha_n^k) = ((\alpha_1, \alpha_2, \ldots, \alpha_{n-1})^k, \alpha_n^k) = ((\alpha_1, \alpha_2, \ldots, \alpha_{n-1}), \alpha_n)^k = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n)^k$. ■

Πόρισμα 1.23. Αν α, β, k θετικοί ακέραιοι, τότε ισχύει η ισοδυναμία: $\alpha \mid \beta \Leftrightarrow \alpha^k \mid \beta^k$.
Απόδειξη: $\alpha \mid \beta \Leftrightarrow (\alpha, \beta) = \alpha \Leftrightarrow (\alpha, \beta)^k = \alpha^k \Leftrightarrow (\alpha^k, \beta^k) = \alpha^k \Leftrightarrow \alpha^k \mid \beta^k$. ■

Πόρισμα 1.24. Αν m θετικός ακέραιος, τότε ο αριθμός $\sqrt[k]{m}$ είναι ρητός αν και μόνον αν το m είναι $k-$στή δύναμη ακεραίου. ($k > 1$.)
Απόδειξη: Έστω $\sqrt[k]{m} = \frac{\alpha}{\beta}$, όπου $\alpha, \beta \in \mathbb{Z}$. Επειδή $\sqrt[k]{m} > 0$, μπορούμε να υποθέσουμε ότι $\alpha, \beta > 0$. Τότε $\frac{\alpha^k}{\beta^k} = m \in \mathbb{Z}$, δηλαδή $\beta^k \mid \alpha^k$. Με βάση το προηγούμενο πόρισμα, $\beta \mid \alpha$. Έστω $\lambda = \frac{\alpha}{\beta} \in \mathbb{Z}$. Τότε $m = \lambda^k$. δηλαδή $\sqrt[k]{m} = \frac{\alpha}{\beta} = \lambda \in \mathbb{Z}$. ■

Για παράδειγμα, οι αριθμοί $\sqrt{2}$, $\sqrt{6}$, $\sqrt[3]{15}$ είναι άρρητοι. Πράγματι, $1^2 = 1 < 2$ και $2^2 = 4 > 2$. Άρα ο $\sqrt{2}$ είναι άρρητος. Παρόμοια ο $\sqrt{6}$ είναι άρρητος γιατί $2^2 = 4 < 6$ και $3^2 = 9 > 6$ και ο $\sqrt[3]{15}$ είναι άρρητος γιατί $2^3 = 8 < 15$ και $3^3 = 27 > 15$.

Πρόταση 1.25. Έστω $\delta_1, \delta_2, \ldots, \delta_n, \alpha > 0$, με $(\delta_i, \delta_j) = 1$, για κάθε i, j με $i \neq j$ και $\delta_1\delta_2 \cdots \delta_n = \alpha^k$, για κάποιον θετικό ακέραιο $k > 1$. Τότε υπάρχουν (μοναδικοί) θετικοί ακέραιοι $x_1, x_2, \ldots, x_n$ τέτοιοι, ώστε $\delta_i = x_i^k$, για κάθε $i = 1, 2, \ldots, n$.
Απόδειξη: Έστω $n = 2$. Θέτουμε $x_1 = (\alpha, \delta_1)$ και $x_2 = (\alpha, \delta_2)$. Τότε $x_1^k = (\alpha, \delta_1)^k = (\alpha^k, \delta_1^k) = (\delta_1\delta_2, \delta_1^k) = \delta_1(\delta_2, \delta_1^{k-1}) = 1$, από το **(i)** του πορίσματος 1.22. Ανάλογα παίρνουμε $x_2^k = \delta_2$. Έστω τώρα $n > 2$. Τότε $\alpha^k = \delta_1\delta$, όπου $\delta = \delta_2 \cdots \delta_n$. Προφανώς $(\delta_1, \delta) = 1$. Εφαρμόζοντας την προηγούμενη περίπτωση, συνάγουμε ότι υπάρχουν $x_1, \beta > 0$ με $x_1^k = \delta_1$ και $\beta^k = \delta = \delta_2 \cdots \delta_n$. Με επαγωγή προκύπτει ότι υπάρχουν $x_2, \ldots, x_n > 0$ τέτοιοι, ώστε $x_i^k = \delta_i$, για κάθε $i = 2, 3, \ldots, n$. ■

Αν $\alpha \in \mathbb{Z}$, θέτουμε $\mathrm{E}(\alpha) = \{\lambda\alpha \mid \lambda \in \mathbb{Z} \text{ και } \lambda\alpha > 0\}$ για το σύνολο των θετικών πολλαπλασίων του α. Αν $\alpha = 0$, τότε $\mathrm{E}(\alpha) = \varnothing$, γιατί το μόνο ακέραιο πολλαπλάσιο του μηδενός είναι το μηδέν. Για το λόγο αυτό στα επόμενα όταν γράφουμε $\mathrm{E}(\alpha)$, θα υποθέτουμε ότι $\alpha \neq 0$.

Ορισμός 1.26. Έστω $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z} \setminus \{0\}$. Το ελάχιστο στοιχείο του $\mathrm{E}(\alpha_1) \cap \mathrm{E}(\alpha_2) \cap \cdots \cap \mathrm{E}(\alpha_n)$ ονομάζεται **ελάχιστο κοινό πολλαπλάσιο των $\alpha_1, \alpha_2, \ldots, \alpha_n$** και συμβολίζεται με $[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

Επειδή $\mathrm{E}(\alpha) = \mathrm{E}(|\alpha|)$, για κάθε $\alpha \in \mathbb{Z} \setminus \{0\}$, θα έχουμε $[\alpha_1, \alpha_2, \ldots, \alpha_n] = [|\alpha_1|, |\alpha_2|, \ldots, |\alpha_n|]$.

Πρόταση 1.27. Αν $\epsilon = [\alpha_1, \alpha_2, \ldots, \alpha_n]$, τότε κάθε κοινό πολλαπλάσιο των $\alpha_1, \alpha_2, \ldots, \alpha_n$ διαιρείται από το ϵ.
Απόδειξη: Έστω ϵ' ένα κοινό πολλαπλάσιο των $\alpha_1, \alpha_2, \ldots, \alpha_n$. Διαιρούμε το ϵ' με το ϵ και παίρνουμε $\epsilon' = \epsilon\pi + \upsilon$, όπου $0 \leq \upsilon < \epsilon$. Εφόσον $\alpha_i \mid \epsilon'$ και $\alpha_i \mid \epsilon$, για κάθε $i = 1, 2, \ldots, n$, έχουμε $\alpha_i \mid \upsilon$, για κάθε $i = 1, 2, \ldots, n$. Άρα το υ είναι κοινό πολλαπλάσιο των $\alpha_1, \alpha_2, \ldots, \alpha_n$ και επειδή το ϵ είναι το ελάχιστο κοινό θετικό πολλαπλάσιο των $\alpha_1, \alpha_2, \ldots, \alpha_n$, θα πρέπει $\upsilon = 0$, ήτοι $\epsilon \mid \epsilon'$. ■

Πρόταση 1.28. Αν $n \geq 3$, $\alpha_1, \alpha_2, \ldots, \alpha_n$ μη μηδενικοί ακέραιοι και $1 < k < n$, τότε
$$[\alpha_1, \alpha_2, \ldots, \alpha_n] = [[\alpha_1, \ldots, \alpha_k], [\alpha_{k+1}, \ldots, \alpha_n]].$$
Απόδειξη: Έστω $\epsilon = [\alpha_1, \alpha_2, \ldots, \alpha_n]$, $\epsilon' = [\epsilon_1, \epsilon_2]$, όπου $\epsilon_1 = [\alpha_1, \ldots, \alpha_k]$ και $\epsilon_2 = [\alpha_{k+1}, \ldots, \alpha_n]$. Εφόσον $\alpha_i \mid \epsilon_1$, για κάθε $i = 1, \ldots, k$, και $\epsilon_1 \mid \epsilon' = [\epsilon_1, \epsilon_2]$, θα έχουμε $\alpha_i \mid \epsilon'$, για κάθε $i = 1, \ldots, k$. Επίσης, $\alpha_i \mid \epsilon_2$, για κάθε $i = k+1, \ldots, n$ και $\epsilon_2 \mid [\epsilon_1, \epsilon_2] = \epsilon'$. Άρα $\alpha_i \mid \epsilon'$, για κάθε $i = 1, 2, \ldots, n$ και κατά συνέπεια $\epsilon = [\alpha_1, \alpha_2, \ldots, \alpha_n] \mid \epsilon'$. Αντιστρόφως, $\alpha_i \mid \epsilon$, για κάθε $i = 1, \ldots, k$. Άρα $\epsilon_1 = [\alpha_1, \ldots, \alpha_k] \mid \epsilon$. Ομοίως $\alpha_i \mid \epsilon$,

για κάθε $i = k+1, \ldots, n$. Άρα $\epsilon_2 = [\alpha_{k+1}, \ldots, \alpha_n] \mid \epsilon$. Αφού $\epsilon_1 \mid \epsilon$ και $\epsilon_2 \mid \epsilon$, έπεται ότι $\epsilon' = [\epsilon_1, \epsilon_2] \mid \epsilon$. Έχουμε λοιπόν $\epsilon \mid \epsilon'$ και $\epsilon' \mid \epsilon$. Άρα $\epsilon = \epsilon'$. ■

Πρόταση 1.29. Έστω $\lambda, \alpha_1, \alpha_2, \ldots, \alpha_n$ μη μηδενικοί ακέραιοι. Τότε
$$[\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_n] = |\lambda| \cdot [\alpha_1, \alpha_2, \ldots, \alpha_n].$$
Απόδειξη: Έστω $\lambda, \alpha_1, \alpha_2, \ldots, \alpha_n > 0$, $\epsilon = [\alpha_1, \alpha_2, \ldots, \alpha_n]$ και $\epsilon' = [\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_n]$. Τότε $\lambda\alpha_i \mid \epsilon' \Leftrightarrow$ $\Leftrightarrow \alpha_i \mid \dfrac{\epsilon'}{\lambda}$, για κάθε $i = 1, 2, \ldots, n$. Επομένως $\epsilon \mid \dfrac{\epsilon'}{\lambda} \Leftrightarrow \lambda\epsilon \mid \epsilon'$. Αντιστρόφως, $\alpha_i \mid \epsilon \Leftrightarrow \lambda\alpha_i \mid \lambda\epsilon$, για κάθε $i = 1, 2, \ldots, n$. Άρα $\epsilon' \mid \lambda\epsilon$. Τελικώς $\epsilon' = \lambda\epsilon$. Στη γενική περίπτωση έχουμε: $[\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_n] =$ $= [|\lambda\alpha_1|, |\lambda\alpha_2|, \ldots, |\lambda\alpha_n|] = |\lambda| \cdot [|\alpha_1|, |\alpha_2|, \ldots, |\alpha_n|] = |\lambda| \cdot [\alpha_1, \alpha_2, \ldots, \alpha_n]$. ■

Στη συνέχεια θα βρούμε έναν τύπο που να συνδέει το ελάχιστο κοινό πολλαπλάσιο δύο αριθμών με τον μέγιστο κοινό διαιρέτη τους.

Θεώρημα 1.30. Έστω $\alpha, \beta \in \mathbb{Z} \setminus \{0\}$. Τότε το ελάχιστο κοινό πολλαπλάσιο των α και β δίνεται από τον τύπο:
$$[\alpha, \beta] = \frac{|\alpha||\beta|}{(\alpha, \beta)}.$$
Απόδειξη: Επειδή $[\alpha, \beta] = [|\alpha|, |\beta|]$, μπορούμε να υποθέσουμε ότι $\alpha, \beta > 0$. Έστω $\delta = (\alpha, \beta)$ και ϵ ένα κοινό πολλαπλάσιο των α και β. Έχουμε $\alpha \mid \epsilon \Leftrightarrow \dfrac{\alpha}{\delta} \mid \dfrac{\epsilon}{\delta}$ και $\beta \mid \epsilon \Leftrightarrow \dfrac{\beta}{\delta} \mid \dfrac{\epsilon}{\delta}$. Επειδή $\left(\dfrac{\alpha}{\delta}, \dfrac{\beta}{\delta}\right) = 1$, σύμφωνα με το **(iii)** της πρότασης 1.21, $\dfrac{\alpha\beta}{\delta^2} = \dfrac{\alpha}{\delta} \cdot \dfrac{\beta}{\delta} \mid \dfrac{\epsilon}{\delta} \Rightarrow \dfrac{\alpha\beta}{\delta} \mid \epsilon$. Επομένως $\epsilon = \kappa \cdot \dfrac{\alpha\beta}{\delta}$, όπου $\kappa \in \mathbb{Z}$. Προφανώς το $\dfrac{\alpha\beta}{\delta} = \alpha \cdot \dfrac{\beta}{\delta} = \dfrac{\alpha}{\delta} \cdot \beta$ είναι κοινό πολλαπλάσιο των α και β. Εφόσον υποθέσαμε ότι $\alpha, \beta > 0$, το $\dfrac{\alpha\beta}{\delta}$ είναι το ελάχιστο (θετικό) κοινό πολλαπλάσιο των α και β και διαιρεί κάθε άλλο κοινό πολλαπλάσιο αυτών.
Στη γενικότερη περίπτωση όπου $\alpha, \beta \neq 0$ παρατηρούμε ότι $[\alpha, \beta] = [|\alpha|, |\beta|] = \dfrac{|\alpha||\beta|}{(|\alpha|, |\beta|)} = \dfrac{|\alpha||\beta|}{(\alpha, \beta)}$. ■

Πόρισμα 1.31. Αν $(\alpha, \beta) = 1$, τότε $[\alpha, \beta] = |\alpha||\beta|$. ■

ΛΥΜΕΝΕΣ ΑΣΚΗΣΕΙΣ

Άσκηση 20. Οι διαιρέσεις των 253 και 525 με έναν θετικό ακέραιο α δίνουν υπόλοιπο 15. Ποιες είναι οι δυνατές τιμές του α;
Λύση: Έχουμε $253 = \alpha\pi_1 + 15$ και $525 = \alpha\pi_2 + 15$. Επομένως $\alpha \mid 253 - 15 = 238$ και $\alpha \mid 525 - 15 = 510$. Επομένως $\alpha \mid (238, 510) = (238, 510 - 2 \cdot 238) = (238, 34) = (7 \cdot 34, 34) = 34 = 2 \cdot 17$. Επειδή $2 < 15$, οι δυνατές τιμές είναι $\alpha = 17$ ή $\alpha = 34$. Πράγματι, $253 = 7 \cdot 34 + 15$ και $525 = 15 \cdot 34 + 15$, άρα και $253 = 14 \cdot 17 + 15$ και $525 = 30 \cdot 17 + 15$. ■

Άσκηση 21. Έστω $\alpha > \beta > 0$. Με την εφαρμογή του ευκλείδειου αλγορίθμου για τον υπολογισμό του (α, β) βρίσκουμε διαδοχικά πηλίκα 1, 2, 1, 20 και 4. Αν $(\alpha, \beta) = 4$, να βρείτε τους α και β.
Λύση: Έχουμε τις σχέσεις:
$$\left.\begin{aligned} \alpha &= \beta + \upsilon_1 \\ \beta &= 2\upsilon_1 + \upsilon_2 \\ \upsilon_1 &= \upsilon_2 + \upsilon_3 \\ \upsilon_2 &= 20\upsilon_3 + \boxed{\upsilon_4} \\ \upsilon_3 &= 4\upsilon_4 \end{aligned}\right\}$$
Το υ_4 είναι λοιπόν ο μέγιστος κοινός διαιρέτης των α και β. Επομένως $\upsilon_4 = 4$. Άρα $\upsilon_3 = 4 \cdot 4 = 16$, $\upsilon_2 = 20 \cdot 16 + 4 = 324$, $\upsilon_1 = 324 + 16 = 340$, $\beta = 2 \cdot 340 + 324 = 1004$ και $\alpha = 1004 + 340 = 1344$. ■

Άσκηση 22. Δείξτε ότι αν $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι ανά δύο πρώτοι μεταξύ τους θετικοί ακέραιοι, τότε
$$[\alpha_1, \alpha_2, \ldots, \alpha_n] = \alpha_1\alpha_2 \cdots \alpha_n.$$
Απόδειξη: Για $n = 2$ η πρόταση ισχύει (πόρισμα 1.31). Έστω ότι ισχύει για $n \geq 2$. Θα δείξουμε ότι

ισχύει για $n+1$. Έστω τώρα $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}$ θετικοί ακέραιοι, ανά δύο πρώτοι μεταξύ τους. Τότε $[\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}] = [[\alpha_1, \alpha_2, \ldots, \alpha_n], \alpha_{n+1}] = [\alpha_1\alpha_2\cdots\alpha_n, \alpha_{n+1}]$, από επαγωγική υπόθεση. Με βάση το **(ii)** της πρότασης 1.21 έχουμε $(\alpha_1\alpha_2\cdots\alpha_n,\ \alpha_{n+1}) = 1$, οπότε η απόδειξη ανάγεται στην περίπτωση $n = 2$. ■

Άσκηση 23. Έστω α, β θετικοί ακέραιοι πρώτοι μεταξύ τους. Τότε $(\alpha+\beta, \alpha-\beta) = 1$ ή 2. Πότε $(\alpha+\beta, \alpha-\beta) = 1$ και πότε $(\alpha+\beta, \alpha-\beta) = 2$;
Απόδειξη: Έστω $\delta = (\alpha+\beta, \alpha-\beta)$. Τότε $\delta \mid (\alpha+\beta)+(\alpha-\beta) = 2\alpha$ και $\delta \mid (\alpha+\beta)-(\alpha-\beta) = 2\beta$. Επομένως $\delta \mid (2\alpha, 2\beta) = 2(\alpha, \beta) = 2$. Άρα $\delta = 1$ ή $\delta = 2$. Επειδή $(\alpha, \beta) = 1$, η περίπτωση και οι δύο να είναι άρτιοι αποκλείεται. Έστω ότι ο ένας είναι άρτιος και ο άλλος περιττός. Τότε οι αριθμοί $\alpha+\beta$ και $\alpha-\beta$ είναι περιττοί. Επομένως και ο μέγιστος κοινός διαιρέτης τους είναι περιττός. Σ' αυτή λοιπόν την περίπτωση προκύπτει ότι $\delta = 1$. Αν και οι δύο είναι περιττοί, τότε οι αριθμοί $\alpha+\beta$ και $\alpha-\beta$ είναι άρτιοι. Το ίδιο και ο μέγιστος κοινός διαιρέτης τους. Άρα, σ' αυτή την περίπτωση $\delta = 2$. ■

Άσκηση 24. Για κάθε $k \geq 1$ οι αριθμοί $6k+5$ και $7k+6$ είναι σχετικώς πρώτοι.
Απόδειξη: Έστω $\delta = (6k+5, 7k+6)$. Τότε $\delta \mid (7k+6)-(6k+5) = k+1$. Άρα $\delta \mid 6(k+1) = 6k+6$. Εφόσον $\delta \mid 6k+5$ και $\delta \mid 6(k+1) = 6k+6$, παίρνουμε $\delta \mid (6k+6)-(6k+5) = 1$. ■

Άσκηση 25. Αν α, β, γ είναι περιττοί, να δείξετε ότι $(\alpha,\ \beta,\ \gamma) = \left(\dfrac{\alpha+\beta}{2}, \dfrac{\beta+\gamma}{2}, \dfrac{\gamma+\alpha}{2}\right)$.

Απόδειξη: Έστω $\delta = (\alpha,\ \beta,\ \gamma)$ και $\delta' = \left(\dfrac{\alpha+\beta}{2}, \dfrac{\beta+\gamma}{2}, \dfrac{\gamma+\alpha}{2}\right)$. Επειδή οι α, β, γ είναι περιττοί, και ο δ είναι περιττός. Τώρα, $\delta \mid \alpha$ και $\delta \mid \beta$. Άρα $\delta \mid \alpha+\beta = 2 \cdot \dfrac{\alpha+\beta}{2}$. Αλλά $(\delta, 2) = 1$. Από το λήμμα του Ευκλείδη, $\delta \,\Big|\, \dfrac{\alpha+\beta}{2}$. Ομοίως $\delta \,\Big|\, \dfrac{\beta+\gamma}{2}$ και $\delta \,\Big|\, \dfrac{\gamma+\alpha}{2}$. Άρα $\delta \mid \delta'$.
Τώρα, $\delta' \,\Big|\, \dfrac{\alpha+\beta}{2}$ και $\delta' \,\Big|\, \dfrac{\beta+\gamma}{2}$. Άρα $\delta' \,\Big|\, \dfrac{\alpha+\beta}{2} - \dfrac{\beta+\gamma}{2} = \dfrac{\alpha-\gamma}{2}$. Επίσης $\delta' \,\Big|\, \dfrac{\gamma+\alpha}{2}$. Επομένως $\delta' \,\Big|\, \dfrac{\gamma+\alpha}{2} + \dfrac{\alpha-\gamma}{2} = \alpha$. Με συμμετρικούς συλλογισμούς συμπεραίνουμε ότι $\delta' \mid \beta$ και $\delta' \mid \gamma$. Επομένως $\delta' \mid (\alpha, \beta, \gamma) = \delta$. ■

Άσκηση 26. Υπενθυμίζουμε ότι ένα κλάσμα $\dfrac{\alpha}{\beta}$ λέγεται **ανάγωγο** αν $(\alpha, \beta) = 1$. Δείξτε ότι για κάθε $n \in \mathbb{Z}$, το κλάσμα $\dfrac{15n^2+8n+6}{30n^2+21n+13}$ είναι ανάγωγο.
Απόδειξη: Κατ' αρχάς παρατηρούμε ότι οι διακρίνουσες των τριωνύμων $15n^2+8n+6$ και $30n^2+21n+13$ είναι αρνητικές και κατά συνέπεια, αφ' ενός ορίζεται το κλάσμα και αφ' ετέρου οι όροι του είναι πάντοτε θετικοί. Έστω $\delta = (15n^2+8n+6, 30n^2+21n+13)$. Έχουμε: $\delta = (15n^2+8n+6, 30n^2+21n+13) =$ $= (30n^2+21n+13-2(15n^2+8n+6), 15n^2+8n+6) = (5n+1, 15n^2+8n+6) = (5n+1, 15n^2+8n+$ $+6-3n(5n+1)) = (5n+1, 5n+6) = (5n+1, 5n+6-(5n+1)) = (5n+1, 5) = (5n+1-5n, 5) = (1, 5) = 1$. ■

Άσκηση 27. Έστω $\alpha, \beta > 0$ και ϵ ένα θετικό κοινό πολλαπλάσιο αυτών. Να δείξετε ότι μια ικανή και αναγκαία συνθήκη για να είναι το ϵ το ελάχιστο κοινό πολλαπλάσιο των α και β είναι η $\left(\dfrac{\epsilon}{\alpha}, \dfrac{\epsilon}{\beta}\right) = 1$.

Απόδειξη: Έστω ότι $\epsilon = [\alpha, \beta] = \dfrac{\alpha\beta}{(\alpha, \beta)}$. Τότε $\dfrac{\epsilon}{\alpha} = \dfrac{\beta}{(\alpha, \beta)}$ και $\dfrac{\epsilon}{\beta} = \dfrac{\alpha}{(\alpha, \beta)}$. Επομένως $\left(\dfrac{\epsilon}{\alpha}, \dfrac{\epsilon}{\beta}\right) =$ $= \left(\dfrac{\beta}{(\alpha, \beta)}, \dfrac{\alpha}{(\alpha, \beta)}\right) = 1$.
Αντιστρόφως, έστω ότι $\left(\dfrac{\epsilon}{\alpha}, \dfrac{\epsilon}{\beta}\right) = 1$. Τότε $\alpha\beta = \alpha\beta\left(\dfrac{\epsilon}{\alpha}, \dfrac{\epsilon}{\beta}\right) = \left(\alpha\beta \cdot \dfrac{\epsilon}{\alpha}, \alpha\beta \cdot \dfrac{\epsilon}{\beta}\right) = (\beta \cdot \epsilon, \alpha \cdot \epsilon) = \epsilon \cdot (\beta, \alpha)$.
Επομένως $\epsilon = \dfrac{\alpha\beta}{(\alpha, \beta)} = [\alpha, \beta]$. ■

Άσκηση 28. Αν $\alpha, \beta > 0$, δείξτε ότι $(\alpha+\beta)[\alpha,\beta] = \beta[\alpha,\alpha+\beta]$.
Απόδειξη: Πρώτα απ' όλα, με βάση την πρόταση 1.11, έχουμε: $(\alpha,\beta) = (\alpha,\alpha+\beta)$. Τώρα, $(\alpha+\beta)[\alpha,\beta] = \frac{(\alpha+\beta)\alpha\beta}{(\alpha,\beta)} = \beta\cdot\frac{(\alpha+\beta)\alpha}{(\alpha,\alpha+\beta)} = \beta[\alpha,\alpha+\beta]$. ■

Άσκηση 29. Αν $\alpha,\beta,\gamma > 0$, δείξτε ότι $[\alpha,\beta,\gamma] = \frac{\alpha\beta\gamma}{(\alpha\beta,\beta\gamma,\gamma\alpha)}$.
Απόδειξη: $[\alpha,\beta,\gamma] = [[\alpha,\beta],\gamma] = \frac{[\alpha,\beta]\gamma}{([\alpha,\beta],\gamma)} = \frac{\alpha\beta\gamma}{(\alpha,\beta)([\alpha,\beta],\gamma)} = \frac{\alpha\beta\gamma}{((\alpha,\beta)[\alpha,\beta],(\alpha,\beta)\gamma)} = \frac{\alpha\beta\gamma}{(\alpha\beta,(\alpha\gamma,\beta\gamma))}$
$= \frac{\alpha\beta\gamma}{(\alpha\beta,\alpha\gamma,\beta\gamma)} = \frac{\alpha\beta\gamma}{(\alpha\beta,\beta\gamma,\gamma\alpha)}$. ■

Άσκηση 30. Έστω $\mathrm{A} = \underbrace{222\ldots2}_{\kappa\ \psi\eta\phi\acute{\iota}\alpha}$ και $\mathrm{B} = \underbrace{888\ldots8}_{\lambda\ \psi\eta\phi\acute{\iota}\alpha}$, τότε $(\mathrm{A},\mathrm{B}) = \frac{2}{9}\cdot(10^{(\kappa,\lambda)}-1)$.
Απόδειξη: Έχουμε $\mathrm{A} = 2\cdot\underbrace{111\ldots1}_{\kappa\ \psi\eta\phi\acute{\iota}\alpha} = 2(10^{\kappa-1}+10^{\kappa-2}+\cdots+10+1) = 2\cdot\frac{10^\kappa-1}{10-1} = \frac{2}{9}\cdot(10^\kappa-1)$. Ομοίως έχουμε $\mathrm{B} = \frac{8}{9}\cdot(10^\lambda-1)$. Προφανώς $9 \mid 10^\kappa-1$ και $9 \mid 10^\lambda-1$. Επομένως $(\mathrm{A},\mathrm{B}) = \frac{1}{9}(2\cdot(10^\kappa-1), 8\cdot(10^\lambda-1)) = \frac{2}{9}(10^\kappa-1, 4\cdot(10^\lambda-1))$. Αλλά το $10^\kappa-1$ είναι περιττός, οπότε $(10^\kappa-1,4)=1$. Από το λήμμα 1.18 προκύπτει ότι $(10^\kappa-1, 4\cdot(10^\lambda-1)) = (10^\kappa-1, 10^\lambda-1)$. Επομένως $(\mathrm{A},\mathrm{B}) = \frac{2}{9}\cdot(10^\kappa-1,10^\lambda-1) = \frac{2}{9}\cdot(10^{(\kappa,\lambda)}-1)$, σύμφωνα με την άσκηση 1.19. ■

Άσκηση 31. Αν $\alpha,\beta,\gamma > 0$, τότε:
(i) Το ελάχιστο κοινό πολλαπλάσιο είναι επιμεριστικό ως προς τον μέγιστο κοινό διαιρέτη, δηλαδή $[(\alpha,\beta),\gamma] = ([\alpha,\gamma],[\beta,\gamma])$.
(ii) Ο μέγιστος κοινός διαιρέτης είναι επιμεριστικός ως προς το ελάχιστο κοινό πολλαπλάσιο, δηλαδή $([\alpha,\beta],\gamma) = [(\alpha,\gamma),(\beta,\gamma)]$.
Απόδειξη: (i) Έστω $\delta = (\alpha,\beta)$. Τότε $[(\alpha,\beta),\gamma] = [\delta,\gamma] = \frac{\delta\gamma}{(\delta,\gamma)} = \frac{\delta\gamma}{(\alpha,\beta,\gamma)}$. Από την άλλη μεριά, θέτουμε $\alpha_1 = \frac{\alpha}{(\alpha,\beta)}$ και $\alpha_1 = \frac{\beta}{(\alpha,\beta)}$. Γνωρίζουμε ότι $(\alpha_1,\beta_1) = 1$. Τώρα, $([\alpha,\gamma],[\beta,\gamma]) = \left(\frac{\alpha\gamma}{(\alpha,\gamma)},\frac{\beta\gamma}{(\beta,\gamma)}\right) = \gamma\left(\frac{\alpha}{(\alpha,\gamma)},\frac{\beta}{(\beta,\gamma)}\right) = \gamma\left(\frac{\alpha_1\delta}{(\alpha_1\delta,\gamma)},\frac{\beta_1\delta}{(\beta_1\delta,\gamma)}\right)$.
Παρατηρούμε ότι $\frac{\alpha_1\delta}{(\alpha_1\delta,\gamma)} = \frac{\alpha_1\frac{\delta}{(\delta,\gamma)}}{\frac{(\alpha_1\delta,\gamma)}{(\delta,\gamma)}} = \frac{\alpha_1\frac{\delta}{(\delta,\gamma)}}{\left(\alpha_1\frac{\delta}{(\delta,\gamma)},\frac{\gamma}{(\delta,\gamma)}\right)}$. Αλλά $\left(\frac{\delta}{(\delta,\gamma)},\frac{\gamma}{(\delta,\gamma)}\right) = 1$. Επομένως $\left(\alpha_1\frac{\delta}{(\delta,\gamma)},\frac{\gamma}{(\delta,\gamma)}\right) = \left(\alpha_1,\frac{\gamma}{(\delta,\gamma)}\right)$. Συνεπώς $\frac{\alpha_1\delta}{(\alpha_1\delta,\gamma)} = \frac{\delta}{(\delta,\gamma)}\frac{\alpha_1}{\left(\alpha_1,\frac{\gamma}{(\delta,\gamma)}\right)} = \frac{\delta}{(\alpha,\beta,\gamma)}\cdot x_1$, όπου $x_1 = \frac{\alpha_1}{\left(\alpha_1,\frac{\gamma}{(\delta,\gamma)}\right)}$. Προφανώς $x_1 \mid \alpha_1$. Ομοίως $\frac{\beta_1\delta}{(\beta_1\delta,\gamma)} = \frac{\delta}{(\alpha,\beta,\gamma)}\cdot y_1$, όπου $y_1 = \frac{\beta_1}{\left(\beta_1,\frac{\gamma}{(\delta,\gamma)}\right)}$. Επίσης, $y_1 \mid \beta_1$. Εφόσον $x_1 \mid \alpha_1$, $y_1 \mid \beta_1$ και $(\alpha_1,\beta_1)=1$, προκύπτει ότι $(x_1,y_1)=1$.
Επομένως $([\alpha,\gamma],[\beta,\gamma]) = \gamma\left(\frac{\alpha_1\delta}{(\alpha_1\delta,\gamma)},\frac{\beta_1\delta}{(\beta_1\delta,\gamma)}\right) = \gamma\left(\frac{\delta}{(\alpha,\beta,\gamma)}\cdot x_1,\frac{\delta}{(\alpha,\beta,\gamma)}\cdot y_1\right) = \frac{\gamma\delta}{(\alpha,\beta,\gamma)}(x_1,y_1) = \frac{\gamma\delta}{(\alpha,\beta,\gamma)}$.
Σημειώνουμε εδώ ότι υπάρχει ο περισσότερο «μπακαλίστικος» αλλά εξίσου αποτελεσματικός και φυσικά

πιο εύκολος τρόπος: $[(\alpha,\beta),\gamma] = ([\alpha,\gamma],[\beta,\gamma]) \Leftrightarrow \dfrac{(\alpha,\beta)\gamma}{(\alpha,\beta,\gamma)} = \left(\dfrac{\alpha\gamma}{(\alpha,\gamma)}, \dfrac{\beta\gamma}{(\beta,\gamma)}\right) \Leftrightarrow \cancel{(\alpha,\beta,\gamma)}(\alpha,\gamma)(\beta,\gamma)$
$\dfrac{(\alpha,\beta)\cancel{\gamma}}{\cancel{(\alpha,\beta,\gamma)}} = (\alpha,\beta,\gamma)(\alpha,\gamma)(\beta,\gamma)\cancel{\gamma}\left(\dfrac{\alpha}{(\alpha,\gamma)}, \dfrac{\beta}{(\beta,\gamma)}\right) \Leftrightarrow (\alpha,\gamma)(\beta,\gamma)(\alpha,\beta) = (\alpha,\beta,\gamma)\left(\cancel{(\alpha,\gamma)}(\beta,\gamma)\dfrac{\alpha}{\cancel{(\alpha,\gamma)}},\right.$
$\left.(\alpha,\gamma)\cancel{(\beta,\gamma)}\dfrac{\beta}{\cancel{(\beta,\gamma)}}\right) \Leftrightarrow (\alpha\beta,\beta\gamma,\alpha\gamma,\gamma^2)(\alpha,\beta) = (\alpha,\beta,\gamma)(\alpha\beta,\alpha\gamma,\alpha\beta,\beta\gamma) = (\alpha,\beta,\gamma)(\alpha\beta,\alpha\gamma,\beta\gamma) \Leftrightarrow$
$\Leftrightarrow (\alpha^2\beta,\alpha\beta\gamma,\alpha^2\gamma,\alpha\gamma^2,\alpha\beta^2,\beta^2\gamma,\alpha\beta\gamma,\beta\gamma^2) = (\alpha^2\beta,\alpha^2\gamma,\alpha\beta\gamma,\alpha\beta^2,\alpha\beta\gamma,\beta^2\gamma,\alpha\beta\gamma,\alpha\gamma^2,\beta\gamma^2) \Leftrightarrow$
$\Leftrightarrow (\alpha^2\beta,\alpha^2\gamma,\beta^2\alpha,\beta^2\gamma,\gamma^2\alpha,\gamma^2\beta,\alpha\beta\gamma) = (\alpha^2\beta,\alpha^2\gamma,\beta^2\alpha,\beta^2\gamma,\gamma^2\alpha,\gamma^2\beta,\alpha\beta\gamma).$

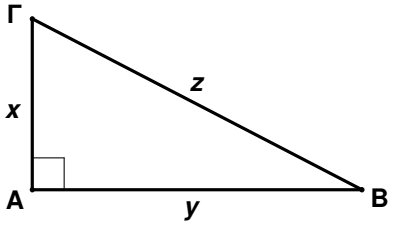
(ii) Έστω $\delta = (\alpha,\beta)$, $\alpha_1 = \dfrac{\alpha}{\delta}$ και $\beta_1 = \dfrac{\beta}{\delta}$. Έχουμε: $([\alpha,\beta],\gamma) = \left(\dfrac{\alpha\beta}{\delta},\gamma\right) = \left(\dfrac{\alpha_1\beta_1\delta^2}{\delta},\gamma\right) = (\alpha_1\beta_1\delta,\gamma) =$
$= (\delta,\gamma)\left(\alpha_1\beta_1\dfrac{\delta}{(\delta,\gamma)}, \dfrac{\gamma}{(\delta,\gamma)}\right) \underset{\left(\frac{\delta}{(\delta,\gamma)},\frac{\gamma}{(\delta,\gamma)}\right)=1}{=} (\alpha,\beta,\gamma)\left(\alpha_1\beta_1, \dfrac{\gamma}{(\delta,\gamma)}\right) \underset{\text{πρόταση 1.21.(iv)}}{=} (\alpha,\beta,\gamma)\left(\alpha_1, \dfrac{\gamma}{(\alpha,\beta,\gamma)}\right)\cdot$
$\left(\beta_1, \dfrac{\gamma}{(\alpha,\beta,\gamma)}\right)$, γιατί προφανώς $(\delta,\gamma) = (\alpha,\beta,\gamma)$.

Από την άλλη μεριά έχουμε: $[(\alpha,\gamma),(\beta,\gamma)] = \dfrac{(\alpha,\gamma)(\beta,\gamma)}{((\alpha,\gamma),(\beta,\gamma))} = \dfrac{(\alpha_1\delta,\gamma)(\beta_1\delta,\gamma)}{(\alpha,\beta,\gamma)} = (\delta,\gamma)^2\dfrac{\frac{(\alpha_1\delta,\gamma)}{(\delta,\gamma)}\frac{(\beta_1\delta,\gamma)}{(\delta,\gamma)}}{(\alpha,\beta,\gamma)} =$
$= (\alpha,\beta,\gamma)\left(\alpha_1\dfrac{\delta}{(\delta,\gamma)}, \dfrac{\gamma}{(\delta,\gamma)}\right)\left(\beta_1\dfrac{\delta}{(\delta,\gamma)}, \dfrac{\gamma}{(\delta,\gamma)}\right) \underset{\left(\frac{\delta}{(\delta,\gamma)},\frac{\gamma}{(\delta,\gamma)}\right)=1}{=} (\alpha,\beta,\gamma)\left(\alpha_1, \dfrac{\gamma}{(\delta,\gamma)}\right)\left(\beta_1, \dfrac{\gamma}{(\delta,\gamma)}\right) =$
$= (\alpha,\beta,\gamma)\left(\alpha_1, \dfrac{\gamma}{(\alpha,\beta,\gamma)}\right)\left(\beta_1, \dfrac{\gamma}{(\alpha,\beta,\gamma)}\right).$

Και η «μπακαλίστικη» λύση: $([\alpha,\beta],\gamma) = [(\alpha,\gamma),(\beta,\gamma)] \Leftrightarrow \left(\dfrac{\alpha\beta}{(\alpha,\beta)},\gamma\right) = \dfrac{(\alpha,\gamma)(\beta,\gamma)}{((\alpha,\gamma),(\beta,\gamma))} \Leftrightarrow \left(\dfrac{\alpha\beta}{(\alpha,\beta)},\gamma\right) =$
$= \dfrac{(\alpha,\gamma)(\beta,\gamma)}{(\alpha,\beta,\gamma)} \Leftrightarrow (\alpha,\beta,\gamma)(\alpha,\beta)\left(\dfrac{\alpha\beta}{(\alpha,\beta)},\gamma\right) = \cancel{(\alpha,\beta,\gamma)}(\alpha,\beta)\dfrac{(\alpha,\gamma)(\beta,\gamma)}{\cancel{(\alpha,\beta,\gamma)}} \Leftrightarrow$
$\Leftrightarrow (\alpha,\beta,\gamma)\left(\cancel{(\alpha,\beta)}\dfrac{\alpha\beta}{\cancel{(\alpha,\beta)}},(\alpha,\beta)\gamma\right) = (\alpha,\beta)(\alpha,\gamma)(\beta,\gamma) \Leftrightarrow (\alpha,\beta,\gamma)(\alpha\beta,\alpha\gamma,\beta\gamma) = (\alpha^2,\alpha\gamma,\beta\alpha,\beta\gamma)(\beta,\gamma) \Leftrightarrow$
$\Leftrightarrow (\alpha^2\beta,\alpha^2\gamma,\alpha\beta\gamma,\alpha\beta^2,\alpha\gamma\beta,\beta^2\gamma,\alpha\beta\gamma,\alpha\gamma^2,\beta\gamma^2) = (\alpha^2\beta,\alpha\gamma\beta,\beta^2\alpha,\beta^2\gamma,\alpha^2\gamma,\alpha\gamma^2,\alpha\beta\gamma,\beta\gamma^2) \Leftrightarrow$
$\Leftrightarrow (\alpha^\beta,\alpha^2\gamma,\beta^2\alpha,\beta^2\gamma,\gamma^2\alpha,\gamma^2\beta,\alpha\beta\gamma) = (\alpha^\beta,\alpha^2\gamma,\beta^2\alpha,\beta^2\gamma,\gamma^2\alpha,\gamma^2\beta,\alpha\beta\gamma).$ ■

Άσκηση 32. (Πυθαγόρειες Τριάδες) Από τα σχολικά μας χρόνια μας είναι γνωστό ίσως το πιο διάσημο Θεώρημα των Μαθηματικών. Το **Πυθαγόρειο Θεώρημα**: Αν έχουμε ένα ορθογώνιο τρίγωνο με κάθετες πλευρές με μήκη x και y και υποτείνουσα με μήκος z, τότε ισχύει η σχέση:

$$\boldsymbol{x^2 + y^2 = z^2} \qquad \textbf{(1)}$$



Σχήμα 1

Τίθεται το ερώτημα: μπορούμε να βρούμε έναν τύπο, ο οποίος να μας δίνει τις πλευρές όλων των ορθογωνίων τριγώνων, όταν τα μήκη των πλευρών είναι ακέραιοι αριθμοί; Με άλλα λόγια μπορούμε να βρούμε όλες τις ακέραιες λύσεις της εξίσωσης $x^2 + y^2 = z^2$;

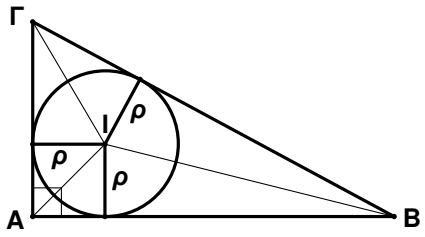
Λύση: Παρατήρηση 1η: Δεν ενδιαφερόμαστε για λύσεις στις οποίες κάποιος από τους x, y και z είναι μηδέν. Αυτές λέγονται τετριμμένες λύσεις και δεν αντιστοιχούν σε τρίγωνο.

Παρατήρηση 2η: Αν θέλουμε και αρνητικές λύσεις, αρκεί να βρούμε τις θετικές. Αν (x,y,z) είναι μια

θετική λύση, τότε και η $(\pm x, \pm y, \pm z)$ είναι επίσης λύση της (1), για όλες τις επιλογές των προσήμων.
Παρατήρηση 3η: Επειδή αν (x, y, z) είναι λύση της (1), τότε και η $(\lambda x, \lambda y, \lambda z)$ είναι λύση της (1), αρκεί να βρούμε τις λύσεις (x, y, z) για τις οποίες ο μέγιστος κοινός διαιρέτης των x, y και z είναι 1. Αυτές λέγονται **πρωταρχικές λύσεις**. Παρατηρούμε τα εξής: Αν $\delta = (x, y, z)$, όπου $x^2 + y^2 = z^2$, τότε $\delta \mid (x, y)$, $\delta \mid (x, z)$ και $\delta \mid (y, z)$. Αντιστρόφως, αν δ' είναι ο μέγιστος κοινός διαιρέτης δύο από τους x, y και z, τότε $\delta' = \delta$. Πράγματι, έστω $\delta' = (x, y)$. Τότε $\delta'^2 = (x^2, y^2) = (x^2, y^2 + x^2) = (x^2, z^2) = (x, z)^2$ και άρα $\delta' = (x, z)$. Άρα $\delta' \mid (x, y, z) = \delta$. Επειδή $\delta \mid \delta'$, έχουμε $\delta = (x, y, z) = (x, y) = \delta'$. Ομοίως, αν $\delta' = (y, z)$, τότε $\delta'^2 = (y^2, z^2) = (y^2, z^2 - y^2) = (y^2, x^2) = (x, y)^2$ και άρα $\delta' = (x, y)$. Άρα $\delta' \mid (x, y, z) = \delta$. Επειδή $\delta \mid \delta'$, έχουμε $\delta = (x, y, z) = (x, y) = \delta'$. Συμπεραίνουμε λοιπόν ότι για να έχουμε μια πρωταρχική τριάδα, αρκεί δύο από τους x, y και z να είναι πρώτοι μεταξύ τους.
Τώρα, για τους παραπάνω λόγους, δεν μπορούν και οι δύο x και y να είναι άρτιοι. Άρα ή είναι και οι δύο περιττοί ή ο ένας άρτιος και ο άλλος περιττός.
Ας εξετάσουμε πρώτα την περίπτωση που και οι δύο x και y είναι περιττοί. Στο παράδειγμα 1.4 (ii) είδαμε ότι το τετράγωνο ενός περιττού είναι της μορφής $8\lambda+1$. Άρα σ' αυτήν την περίπτωση $x^2+y^2 = 8\lambda+1+8\lambda'+1 = 2(4(\lambda+\lambda')+1)$. Ο $z^2 = x^2 + y^2$ είναι αναγκαστικά άρτιος, άρα και ο z. Έστω $z = 2r$. Τότε $z^2 = 4r^2$. Επομένως θα έχουμε $2(4(\lambda+\lambda')+1) = 4r^2 \Leftrightarrow 4(\lambda+\lambda')+1 = 2r^2$, δηλαδή περιττός ίσον άρτιος, άτοπο.
Συμπέρασμα: Ο ένας από τους x, y είναι περιττός και ο άλλος άρτιος. Τότε ο $z^2 = x^2 + y^2$ θα είναι περιττός, άρα και ο z περιττός. Ας συμφωνήσουμε ο x να είναι περιττός και ο y άρτιος. Έστω $y = 2\rho$. Τότε $y^2 = z^2 - x^2 \Leftrightarrow 4\rho^2 = (z+x)(z-x)$ και επειδή οι $z+x$, $z-x$ είναι άρτιοι ως άθροισμα και διαφορά περιττών αντίστοιχα, θα έχουμε $\rho^2 = \dfrac{z+x}{2} \cdot \dfrac{z-x}{2}$. Αν $\delta = \left(\dfrac{z+x}{2}, \dfrac{z-x}{2}\right)$, τότε $\delta \,\Big|\, \dfrac{z+x}{2} + \dfrac{z-x}{2} = z$ και $\delta \,\Big|\, \dfrac{z+x}{2} - \dfrac{z-x}{2} = x$. Επομένως $\delta \mid (x, z) = 1$. Με βάση την πρόταση 1.25, το ρ γράφεται στη μορφή mn, όπου $m^2 = \dfrac{z+x}{2}$ και $n^2 = \dfrac{z-x}{2}$. Επομένως $x = \dfrac{z+x}{2} - \dfrac{z-x}{2} = m^2 - n^2$ και $z = \dfrac{z+x}{2} + \dfrac{z-x}{2} = m^2 + n^2$.
Συμπέρασμα: $x = m^2 - n^2$, $y = 2mn$ και $z = m^2 + n^2$. Επίσης $m > n$ για να είναι $x > 0$. Ακόμη, για να είναι ο x περιττός, θα πρέπει ο ένας από τους m και n να είναι άρτιος και ο άλλος περιττός. Επιπροσθέτως, για να είναι $(x, z) = 1$ θα πρέπει $(m, n) = 1$. Πράγματι, αν $d = (m, n)$, τότε $d^2 \mid m^2$ και $d^2 \mid n^2$. Άρα $d^2 \mid m^2 - n^2 = x^2$ και $d^2 \mid m^2 + n^2 = z^2$. Κατά συνέπεια, (πόρισμα 1.23) $d \mid x$ και $d \mid z$, άρα $d \mid (x, z)$. Αναγκαστικά λοιπόν $d = (m, n) = 1$. Αντίστροφα, έστω $(m, n) = 1$. Τότε και $(m^2, n^2) = 1$. Αν $d = (x, z) = (m^2 - n^2, m^2 + n^2)$, τότε $d \mid (m^2 - n^2) + (m^2 + n^2) = 2m^2$ και $d \mid (m^2 + n^2) - (m^2 - n^2) = 2n^2$. Άρα $d \mid (2m^2, 2n^2) = 2 \cdot (m^2, n^2) = 2$. Επειδή οι x και z είναι περιττοί και το d θα πρέπει να είναι περιττός. Επομένως $d = (x, z) = 1$. Από όλα τα παραπάνω προκύπτει το εξής συμπέρασμα:
Οι θετικές πρωταρχικές λύσεις της εξίσωσης $x^2 + y^2 = z^2$ είναι της μορφής: $x = m^2 - n^2$, $y = 2mn$ και $z = m^2 + n^2$, όπου $m > n$, $(m, n) = 1$ και ο ένας από τους m, n είναι άρτιος και ο άλλος περιττός.
Σημειώνουμε εδώ ότι θα μπορούσαμε να εναλλάξουμε τις κάθετες πλευρές x και y του ορθογωνίου τριγώνου και να πάρουμε $x = 2mn$, $y = m^2 - n^2$ και $z = m^2 + n^2$, αλλά κάτι τέτοιο είναι μάλλον άχρηστο αφού τα τρίγωνα παραμένουν ίσα. Τελικό συμπέρασμα:
Οι ακέραιες πλευρές ενός ορθογωνίου τριγώνου δίνονται από τους τύπους $x = t(m^2 - n^2)$, $y = 2tmn$ και $z = t(m^2 + n^2)$, όπου $t > 0$, $m > n$, $(m, n) = 1$ και ένας εκ των m και n είναι άρτιος και ο άλλος περιττός. ■

Παράδειγμα 1.32. (i) Αν θέσουμε $m = 7$ και $n = 2$, θα πάρουμε $x = 7^2 - 2^2 = 45$, $y = 2 \cdot 7 \cdot 2 = 28$ και $z = 7^2 + 2^2 = 53$. Τότε $x^2 + y^2 = 45^2 + 28^2 = 2025 + 784 = 2809 = 53^2 = z^2$.
(ii) Αν θέσουμε $m = 8$ και $n = 3$, θα πάρουμε $x = 8^2 - 3^2 = 55$, $y = 2 \cdot 8 \cdot 3 = 48$ και $z = 8^2 + 3^2 = 73$. Τότε $x^2 + y^2 = 55^2 + 48^2 = 3025 + 2304 = 5329 = 73^2 = z^2$.
(iii) Αν θέσουμε $m = 10$ και $n = 9$, θα πάρουμε $x = 10^2 - 9^2 = 19$, $y = 2 \cdot 10 \cdot 9 = 180$ και $z = 10^2 + 9^2 = 181$. Τότε $x^2 + y^2 = 19^2 + 180^2 = 361 + 32400 = 32761 = 181^2 = z^2$. ■

Άσκηση 33. Δίνεται ένα ορθογώνιο τρίγωνο ΑΒΓ ($\hat{A} = 90^o$), του οποίου οι πλευρές έχουν ακέραια μήκη. Τότε και το μήκος της ακτίνας ρ του εγγεγραμμένου κύκλου είναι ακέραιος.



Σχήμα 2

Απόδειξη: Το εμβαδόν Ε του τριγώνου ΑΒΓ ισούται με το ημιγινόμενο των καθέτων πλευρών, ήτοι $\mathrm{E} = \frac{1}{2}t(m^2-n^2)2tmn = 2t^2(m^2-n^2)mn$, όπου t, m, n όπως προηγουμένως. Επίσης, $\mathrm{E} = \rho\tau$, όπου $\tau = \frac{1}{2}(t(m^2-n^2)+2tmn+t(m^2+n^2)) = tm(m+n)$ η ημιπερίμετρος αυτού.
Επομένως $\rho = \dfrac{2t^2(m^2-n^2)mn}{tm(m+n)} = 2tn(m-n) \in \mathbb{Z}$. ■

Άσκηση 34. Αν n θετικός ακέραιος και k θετικός περιττός ακέραιος, τότε
$$1+2+3+\cdots+n \mid 1^k+2^k+3^k+\cdots+n^k.$$
Απόδειξη: Ως γνωστόν $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$. Θέτουμε $\mathrm{S}_n = 1^k+2^k+3^k+\cdots+n^k$. Παρατηρούμε ότι $2\mathrm{S}_n = (1^k+n^k)+(2^k+(n-1)^k)+(3^k+(n-2)^k)+\cdots+(n^k+1^k)$. Κάθε παρένθεση είναι της μορφής $\mu^k+(n-\mu+1)^k$, όπου $\mu = 1,2,\ldots,n$. Επειδή το k περιττός, έχουμε $\mu^k+(n-\mu+1)^k = (\mu+n-\mu+1)\big(\mu^{k-1}-\mu^{k-2}(n-\mu+1)+\mu^{k-3}(n-\mu+1)^2-\cdots+(n-\mu+1)^{k-1}\big) = (n+1)\cdot\mathrm{A}_\mu$, όπου A_μ η αντίστοιχη παρένθεση. Επομένως $n+1 \mid 2\mathrm{S}_n$, για κάθε θετικό n. Παρατηρούμε επίσης ότι $1 \mid 2\mathrm{S}_1$. Υποθέτουμε ότι $n \geq 2$. Τότε $n = (n-1)+1 \mid \mathrm{S}_{n-1}$ και $2\mathrm{S}_n = 2\mathrm{S}_{n-1}+2n^k$. Εφόσον $n \mid \mathrm{S}_{n-1}$, έπεται ότι $n \mid 2\mathrm{S}_n$. Επειδή $n, n+1 \mid 2\mathrm{S}_n$ και $(n, n+1) = 1$, έπεται ότι $n(n+1) \mid 2\mathrm{S}_n \Leftrightarrow \dfrac{n(n+1)}{2} \,\Big|\, \mathrm{S}_n$. ■

ΑΛΥΤΕΣ ΑΣΚΗΣΕΙΣ

19. Έστω $(\alpha,\beta) = 1$ και $\alpha x+\beta y = 1$. Ποιος είναι ο μέγιστος κοινός διαιρέτης των x και y;

20. Αληθεύει ότι αν $r \mid s+t$ και $(s,t) = 1$, τότε $(r,s) = (r,t) = 1$;

21. Βρείτε τους ακόλουθους μέγιστους κοινούς διαιρέτες: $(143, 227)$, $(306, 657)$ και $(272, 1479)$.

22. Χρησιμοποιώντας τον ευκλείδειο αλγόριθμο, βρείτε $x, y \in \mathbb{Z}$ τέτοιους, ώστε:
(i) $(56, 72) = 56x+72y$.
(ii) $(24, 138) = 24x+138y$.
(ii) $(651, 395) = 651x+395y$.
(iv) $(1769, -2378) = 1769x+(-2378)y$.

23. Υποθέτουμε ότι $(\alpha,\beta) = 1$. Αποδείξτε τα ακόλουθα:
(i) $(2\alpha+\beta, \alpha+2\beta) = 1$ ή 3.
(ii) $(\alpha+\beta, \alpha^2+\beta^2) = 1$ ή 2.
(iii) $(\alpha+\beta, \alpha^2-\alpha\beta+\beta^2) = 1$ ή 3.
(iv) $(\alpha^2-\beta^2, 2\alpha\beta) = 1$ ή 2.

24. Έστω $\alpha > 1$ και m, n θετικοί ακέραιοι. Δείξτε ότι ισχύει η ισοδυναμία
$$[\alpha^m-1, \alpha^n-1] = \alpha^{[m,n]}-1 \Leftrightarrow \big(m \mid n \text{ ή } n \mid m\big).$$

25. Αν α, β είναι μη μηδενικοί ακέραιοι, τότε $(\alpha,\beta) = [\alpha,\beta]$ αν και μόνον αν $\alpha = \pm\beta$.

26. Να βρεθούν ακέραιοι x, y, z τέτοιοι, ώστε:
(i) $(147, 28, 6) = 147x+28y+6z$.
(ii) $(198, 288, 512) = 198x+288y+512z$.

27. Να δείξετε ότι για κάθε $\kappa \in \mathbb{Z}$ το κλάσμα $\dfrac{\kappa^2+3\kappa+2}{2\kappa+3}$ είναι ανάγωγο.

28. Έστω $f_1 = f_2 = 1$, $f_3 = 2$, $f_4 = 3$, $f_5 = 5$, $f_6 = 8$,...,$f_{n+2} = f_{n+1} + f_n$,... η ακολουθία του Fibonacci. Δείξτε ότι $(f_n, f_{n+1}) = 1$, για κάθε $n = 1, 2, \ldots$

29. Να βρεθεί ο $(n! + 1, (n + 1)! + 1)$, όπου n θετικός ακέραιος.

30. Αληθεύει ότι αν $(r, s) = (u, v) = 1$ και $\dfrac{r}{s} + \dfrac{u}{v} \in \mathbb{Z}$, τότε $s = \pm v$;

31. Έστω k θετικός ακέραιος. Να βρεθεί ο μέγιστος κοινός διαιρέτης των αριθμών $5k - 4$ και $9k - 7$.

32. Δείξτε ότι αν $\alpha\beta' - \alpha'\beta = \pm 1$, τότε $(\alpha + \alpha', \beta + \beta') = 1$.

33. Δείξτε ότι $(\alpha, \beta) = (\alpha + \beta, [\alpha, \beta])$

34. Να βρείτε τους ακεραίους αριθμούς α, β για τους οποίους ισχύουν: $(\alpha, \beta) = 12$, $[\alpha, \beta] = 420$ και $20 < \alpha < \beta$.

35. Έστω x, y, α, β θετικοί ακέραιοι. Υποθέτουμε ότι $(\alpha, \beta) = 1$ και $x^\alpha = y^\beta$. Δείξτε ότι υπάρχει θετικός ακέραιος n τέτοιος, ώστε $x = n^\beta$ και $y = n^\alpha$.

36. Να βρείτε όλους τους θετικούς ακεραίους αριθμούς x, y, με $x \le y$ και $x + y - 1 = [x, y]$.

37. Δείξτε ότι $(\alpha\kappa, \beta\lambda) = (\alpha, \beta)(\kappa, \lambda)\left(\dfrac{\alpha}{(\alpha,\beta)}, \dfrac{\kappa}{(\kappa,\lambda)}\right)\left(\dfrac{\beta}{(\alpha,\beta)}, \dfrac{\lambda}{(\kappa,\lambda)}\right)$.

1.3 Πρώτοι Αριθμοί

Ορισμός 1.33. Ένας θετικός ακέραιος μεγαλύτερος του 1 λέγεται **πρώτος**, αν οι μοναδικοί θετικοί διαιρέτες του είναι το 1 και ο εαυτός του. Ένας θετικός ακέραιος μεγαλύτερος του 1, ο οποίος δεν είναι πρώτος, λέγεται **σύνθετος**.

Για παράδειγμα, οι αριθμοί, 2, 3, 5, 7, 11, 13, 17, 19 κτλ, είναι πρώτοι, ενώ οι αριθμοί 4, 6, 8, 9, 10, 12, 14, 15 κτλ, είναι σύνθετοι. Είναι σαφές ότι ο μοναδικός άρτιος πρώτος είναι το 2. Από τον ορισμό των πρώτων αριθμών προκύπτει το επόμενο συμπέρασμα:

Πρόταση 1.34. Έστω $\alpha \in \mathbb{Z}$ και p, q πρώτοι. Τότε

(i) $(\alpha, p) = \begin{cases} p, & \text{αν } p \mid \alpha \\ 1, & \text{αν } p \nmid \alpha \end{cases}$ **(ii)** Ισχύει η ισοδυναμία $p \mid q \Leftrightarrow p = q$.

(iii) Αν $p \mid \alpha$, $q \mid \beta$ και $(\alpha, \beta) = 1$, τότε $p \neq q$.

Απόδειξη: **(i)** Έστω $\delta = (\alpha, p)$. Τότε $\delta \mid p$ και επειδή ο p είναι πρώτος, $\delta = 1$ ή $\delta = p$. Στη δεύτερη περίπτωση παίρνουμε $p \mid \alpha$.
(ii) Αν $p \mid q$ και $p \neq q$, τότε το q δεν θα ήταν πρώτος, αφού θα είχε και άλλον διαιρέτη εκτός του 1 και του εαυτού του.
(iii) Αν $p = q$, τότε θα είχαμε $p \mid \alpha$ και $p \mid \beta$. Άρα $p \mid (\alpha, \beta) = 1$, άτοπο. ■

Πόρισμα 1.35. Αν p πρώτος και $p \mid \alpha_1\alpha_2 \cdots \alpha_n$, τότε $p \mid \alpha_i$, για κάποιο $i = 1, 2, \ldots, n$.
Απόδειξη: Για $n = 1$, η πρόταση είναι τετριμμένη. Έστω $n > 1$. Αν $p \mid \alpha_1$, έχει καλώς. Αν όχι, τότε με βάση το (i) της πρότασης 1.34, $(p, \alpha_1) = 1$, Άρα, με βάση το λήμμα του Ευκλείδη (λήμμα 1.17), $p \mid \alpha_2 \cdots \alpha_n$. Το αποτέλεσμα προκύπτει με επαγωγή επί του n. ■

Θα αποδείξουμε ότι κάθε θετικός ακέραιος μεγαλύτερος του 1 αναλύεται κατά μοναδικό τρόπο σε γινόμενο πρώτων αριθμών. Ξεκινάμε με το επόμενο λήμμα:

Λήμμα 1.36. Κάθε θετικός ακέραιος $\alpha > 1$ έχει έναν πρώτο διαιρέτη.
Απόδειξη: Για $\alpha = 2$, ο ίδιος ο 2 είναι πρώτος διαιρέτης του εαυτού του. Έστω ότι το λήμμα ισχύει για όλους τους ακεραίους β με $1 < \beta < \alpha$. Θα δείξουμε ότι και ο α έχει έναν πρώτο διαιρέτη. Αν ο α είναι πρώτος, τότε ο ίδιος είναι διαιρέτης του εαυτού του. Έστω λοιπόν ότι ο α δεν είναι πρώτος, άρα σύνθετος. Τότε ο α έχει γνήσιους διαιρέτες, διαφορετικούς της μονάδας, δηλαδή το σύνολο Α$= \{d \in \mathbb{Z} |\ 1 < d < \alpha$ και $d \mid \alpha\}$ δεν είναι κενό. Προφανώς είναι κάτω φραγμένο (από το 2) και κατά συνέπεια έχει (μοναδικό) ελάχιστο στοιχείο, το οποίο συμβολίζουμε με p. Θα δείξουμε ότι ο p είναι πρώτος. Από τον ορισμό του συνόλου Α έχουμε $1 < p$. Αν ο p είχε κάποιον διαιρέτη, ας πούμε k, με $1 < k < p$, τότε ο k θα ήταν διαιρέτης και του α, άρα $k \in$ Α, άτοπο γιατί ο p είναι το ελάχιστο στοιχείο του συνόλου Α. ■

Πόρισμα 1.37. Δύο ακέραιοι α, β μεγαλύτεροι του 1, είναι πρώτοι μεταξύ τους αν και μόνον αν έχουν διαφορετικούς πρώτους διαιρέτες. Γενικότερα, δύο ακέραιοι α, β με $|\alpha| \geq 2$ και $|\beta| \geq 2$ είναι πρώτοι μεταξύ τους αν και μόνον αν έχουν διαφορετικούς πρώτους διαιρέτες.
Απόδειξη: Έστω $\alpha, \beta > 1$. Αν $(\alpha, \beta) = 1$, τότε οι α και β έχουν διαφορετικούς πρώτους διαιρέτες, σύμφωνα με το (iii) της πρότασης 1.34. Αντιστρόφως, υποθέτουμε ότι οι α και β έχουν διαφορετικούς πρώτους διαιρέτες. Έστω $\delta = (\alpha, \beta)$. Αν $\delta > 1$, τότε ο δ θα είχε έναν πρώτο διαιρέτη p. Επειδή ο δ διαιρεί και τον α και τον β και ο p διαιρεί τον δ, ο p θα διαιρούσε και τον α και τον β. Άτοπο. Η γενικότερη περίπτωση προκύπτει από τη σχέση $(\alpha, \beta) = (|\alpha|, |\beta|)$. ■

Λήμμα 1.38. Κάθε θετικός ακέραιος $\alpha > 1$ αναλύεται σε γινόμενο πρώτων παραγόντων.
Απόδειξη: Αν ο α ήταν κάποιος πρώτος p, τότε η «ανάλυση» $\alpha = p$ είναι η τετριμμένη (αποδεκτή όμως) ανάλυση, με πλήθος παραγόντων 1. Μια τέτοια περίπτωση είναι η $\alpha = 2$.
Έστω ότι ο α είναι σύνθετος. Με βάση το λήμμα 1.36, ο α έχει έναν πρώτο διαιρέτη p_1. Άρα $\alpha = p_1\alpha'$, όπου α' θετικός ακέραιος. Εφόσον ο α είναι σύνθετος, $1 < \alpha' < \alpha$. Με επαγωγή επί του α συνάγουμε ότι ο α' αναλύεται σε γινόμενο πρώτων, δηλαδή $\alpha' = p_2 \cdots p_n$, όπου p_i πρώτος για κάθε $i = 2, \ldots, n$. Άρα $\alpha = p_1 p_2 p_3 \cdots p_n$. ■

Θεώρημα 1.39. (Θεμελιώδες Θεώρημα της Αριθμητικής) Κάθε ακέραιος $\alpha > 1$ αναλύεται κατά τρόπο **μοναδικό** σε γινόμενο πρώτων παραγόντων. Δηλαδή, αν $\alpha = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, όπου n, m θετικοί ακέραιοι και $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_m$ πρώτοι, με $p_1 \leq p_2 \leq \ldots \leq p_n$ και $q_1 \leq q_2 \leq \ldots \leq q_m$, τότε $n = m$ και $p_i = q_i$, για κάθε $i = 1, 2, \ldots, n$.
Απόδειξη: Για $n = 1$ θα είχαμε: $p_1 = q_1 q_2 \cdots q_m$ (1). Τότε και $m = 1$, αλλιώς το δεύτερο μέλος της σχέσεως (1) θα ήταν σύνθετος αριθμός. Άρα $p_1 = q_1$. Ομοίως, αν $m = 1$, τότε και $n = 1$.
Έστω τώρα ότι $n > 1$ και $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$. Επειδή $p_1 \mid q_1 q_2 \cdots q_m$, από το πόρισμα 1.35 προκύπτει ότι $p_1 \mid q_j$, για κάποιο $j = 1, 2, \ldots, m$. Επομένως $p_1 = q_j \geq q_1$. Ομοίως, $q_1 = p_i \geq p_1$, για κάποιο $i = 1, 2, \ldots, n$. Άρα: $p_1 = q_j \geq q_1 = p_i \geq p_1$. Συνεπώς $p_1 = q_1$ και άρα $p_2 \cdots p_n = q_2 \cdots q_m$. Η απόδειξη ολοκληρώνεται με επαγωγή επί του n. ■

Συμπεράσματα: **1ο**: Αν ομαδοποιήσουμε τους ίσους πρώτους, προκύπτει ότι κάθε ακέραιος $\alpha > 1$ γράφεται μονοσήμαντα στη μορφή $\alpha = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, όπου $k = 1, 2, \ldots$, $p_i < p_j$ για κάθε $i < j$ και $r_i > 0$, για κάθε $i = 1, 2, \ldots, k$.
2ο: Μερικές φορές είναι βολικό να «συμπληρώνουμε» τη γραφή $p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ στην ανάλυση ενός ακεραίου με κάποια $r_i = 0$. Αυτό δεν επηρεάζει το τελικό αποτέλεσμα, αφού σ' αυτήν την περίπτωση θα είναι $p_i^{r_i} = p_i^0 = 1$. Αυτό συνήθως γίνεται όταν θεωρούμε δύο ακεραίους για τους οποίους δεν ξέρουμε αν έχουν τους ίδιους πρώτους διαιρέτες.
3ο: Πολλές φορές δεν μας ενδιαφέρει η διάταξη των πρώτων διαιρετών. Γράφουμε απλώς $\alpha = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, όπου $p_i \neq p_j$ για κάθε $i, j \in \{1, 2, \ldots, k\}$ με $i \neq j$.

Πόρισμα 1.40. Κάθε ακέραιος $\alpha \in \mathbb{Z} \setminus \{-1, 0, 1\}$ γράφεται μονοσήμαντα (αν αδιαφορήσουμε για τη διάταξη των πρώτων διαιρετών του) στη μορφή $\alpha = \epsilon \cdot p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, $(k = 1, 2, \ldots)$ με $p_i \neq p_j$ για κάθε $i \neq j$ και $r_i > 0$, για κάθε $i = 1, 2, \ldots, k$ και $\epsilon = \begin{cases} 1, & \text{αν } \alpha > 1 \\ -1, & \text{αν } \alpha < -1 \end{cases}$ ■

Σημειώνουμε εδώ ότι και το ± 1 μπορεί να γραφεί στην ανωτέρω μορφή, αν θέσουμε $r_1 = r_2 = \cdots = r_k = 0$.

Λήμμα 1.41. Έστω $\alpha = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ και $\beta = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, p_i διαφορετικοί πρώτοι και $0 \leq r_i, s_i$, για κάθε $i = 1, 2, \ldots, k$. Τότε ικανή και αναγκαία συνθήκη για να είναι ο α διαιρέτης του β είναι $r_i \leq s_i$, για κάθε $i = 1, 2, \ldots, k$.
Απόδειξη: Αν $r_i \leq s_i$, για κάθε $i = 1, 2, \ldots, k$, τότε $\beta = \alpha \cdot \lambda$, όπου $\lambda = p_1^{s_1 - r_1} p_2^{s_2 - r_2} \cdots p_k^{s_k - r_k} \in \mathbb{Z}$. Αντιστρόφως, υποθέτουμε ότι $\alpha \mid \beta$. Τότε $\beta = \lambda\alpha$, για κάποιο $\lambda \in \mathbb{Z}$. Επομένως $p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} = \lambda p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. Αν $r_i > s_i$, για κάποιο i, τότε $p_1^{s_1} \cdots p_{i-1}^{s_{i-1}} p_{i+1}^{s_{i+1}} \cdots p_k^{s_k} = \lambda p_1^{r_1} \cdots p_{i-1}^{r_{i-1}} \cdot p_i^{r_i - s_i} \cdot p_{i+1}^{r_{i+1}} \cdots p_k^{r_k}$. Αλλά τότε $p_i \mid p_1^{s_1} \cdots p_{i-1}^{s_{i-1}} p_{i+1}^{s_{i+1}} \cdots p_k^{s_k}$, άτοπο γιατί $p_i \neq p_j$, για κάθε $j \in \{1, \ldots, i-1, i+1, \ldots, k\}$. ■

Πρόταση 1.42. Έστω $\alpha = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ και $\beta = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, όπου p_i διαφορετικοί πρώτοι και $r_i, s_i \geq 0$, για κάθε $i = 1, 2, \ldots, k$. Τότε:
(i) $(\alpha, \beta) = p_1^{\min\{r_1, s_1\}} p_2^{\min\{r_2, s_2\}} \cdots p_k^{\min\{r_k, s_k\}}$ και **(ii)** $[\alpha, \beta] = p_1^{\max\{r_1, s_1\}} p_2^{\max\{r_2, s_2\}} \cdots p_k^{\max\{r_k, s_k\}}$.
Απόδειξη: Επειδή μπορούμε να προσθέσουμε με μηδενικούς εκθέτες όσους p_i λείπουν, μπορούμε να υποθέσουμε ότι ένας κοινός διαιρέτης δ των α και β έχει τη μορφή $\delta = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ και ένα κοινό πολλαπλάσιο ϵ των α και β τη μορφή $\epsilon = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}$, όπου $t_i, u_i \geq 0$, για κάθε $i = 1, 2, \ldots, k$.
(i) Σύμφωνα με το προηγούμενο λήμμα, εφόσον $\delta \mid \alpha$ και $\delta \mid \beta$, θα πρέπει $t_i \leq r_i$ και $t_i \leq s_i$ και άρα $t_i \leq \min\{t_i, s_i\}$, για κάθε $i = 1, 2, \ldots, k$. Επομένως $\delta \mid p_1^{\min\{r_1, s_1\}} p_2^{\min\{r_2, s_2\}} \cdots p_k^{\min\{r_k, s_k\}} = d$. Πάλι με βάση το προηγούμενο λήμμα και επειδή $\min\{t_i, s_i\} \leq t_i$ και $\min\{t_i, s_i\} \leq s_i$, ο d είναι κοινός διαιρέτης των α και β, ο οποίος όπως δείξαμε διαιρείται από κάθε κοινό διαιρέτη των α και β. Συνεπώς $d = (\alpha, \beta)$.
(ii) Σύμφωνα με το προηγούμενο λήμμα, εφόσον $\alpha \mid \epsilon$ και $\beta \mid \epsilon$, θα πρέπει $r_i \leq u_i$ και $s_i \leq u_i$ και άρα $\max\{r_i, s_i\} \leq u_i$, για κάθε $i = 1, 2, \ldots, k$. Επομένως $e = p_1^{\max\{r_1, s_1\}} p_2^{\max\{r_2, s_2\}} \cdots p_k^{\max\{r_k, s_k\}} \mid \epsilon$. Πάλι με βάση το προηγούμενο λήμμα και επειδή $\max\{t_i, s_i\} \leq t_i$ και $\max\{t_i, s_i\} \leq s_i$, το e είναι κοινό πολλαπλάσιο των α και β, το οποίο όπως δείξαμε διαιρεί κάθε κοινό πολλαπλάσιο των α και β. Συνεπώς $e = [\alpha, \beta]$. ■

Παράδειγμα 1.43. Ας υποθέσουμε ότι $\alpha = 3^2 \cdot 7^3 \cdot 11 \cdot 37^3$ και $\beta = 2^4 \cdot 11^3 \cdot 23 \cdot 37$. Γράφουμε $\alpha = 2^0 \cdot 3^2 \cdot 7^3 \cdot 11^1 \cdot 23^0 \cdot 37^3$ και $\beta = 2^4 \cdot 3^0 \cdot 7^0 \cdot 11^3 \cdot 23^1 \cdot 37^1$. Τότε $(\alpha, \beta) = 2^{\min\{0,4\}} \cdot 3^{\min\{2,0\}} \cdot 7^{\min\{3,0\}} \cdot 11^{\min\{1,3\}} \cdot 23^{\min\{0,1\}} \cdot 37^{\min\{3,1\}} = 2^0 \cdot 3^0 \cdot 7^0 \cdot 11^1 \cdot 23^0 \cdot 37^1 = 11 \cdot 37 = 407$.
Επίσης, $[\alpha, \beta] = 2^{\max\{0,4\}} \cdot 3^{\max\{2,0\}} \cdot 7^{\max\{3,0\}} \cdot 11^{\max\{1,3\}} \cdot 23^{\max\{0,1\}} \cdot 37^{\max\{3,1\}} = 2^4 \cdot 3^2 \cdot 7^3 \cdot 11^3 \cdot 23^1 \cdot 37^3 = 16 \cdot 9 \cdot 343 \cdot 1331 \cdot 23 \cdot 50653 = 76589225154288$.

Το παραπάνω παράδειγμα δικαιολογεί τον εμπειρικό κανόνα που μάθαμε στο δημοτικό. *¨Αν θέλουμε να υπολογίσουμε του μέγιστο κοινό διαιρέτη δύο αριθμών, παίρνουμε μόνον τους κοινούς πρώτους παράγοντες στη μικρότερη δύναμη¨*. Επίσης, *¨αν θέλουμε να υπολογίσουμε το ελάχιστο κοινό πολλαπλάσιο δύο αριθμών παίρνουμε όλους τους πρώτους παράγοντες (κοινούς και μη κοινούς) στη μεγαλύτερη δύναμη¨*.

Με βάση επίσης την παραπάνω πρόταση, μπορούμε να δώσουμε μια άλλη απόδειξη του τύπου $(\alpha, \beta)[\alpha, \beta] = \alpha\beta$, όπου α και β είναι θετικοί ακέραιοι. Αυτό στηρίζεται στην απλή σχέση $\min\{x, y\} + \max\{x, y\} = x + y$, για κάθε $x, y \in \mathbb{R}$.
Πράγματι, έστω $\alpha = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ και $\beta = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, όπου p_i διαφορετικοί πρώτοι και $r_i, s_i \geq 0$, για κάθε $i = 1, 2, \ldots, k$. Τότε $(\alpha, \beta)[\alpha, \beta] = \left(p_1^{\min\{r_1, s_1\}} p_2^{\min\{r_2, s_2\}} \cdots p_k^{\min\{r_k, s_k\}}\right) \cdot \left(p_1^{\max\{r_1, s_1\}} p_2^{\max\{r_2, s_2\}} \cdots p_k^{\max\{r_k, s_k\}}\right) =$
$= p_1^{\min\{r_1, s_1\} + \max\{r_1, s_1\}} p_2^{\min\{r_2, s_2\} + \max\{r_2, s_2\}} \cdots p_k^{\min\{r_k, s_k\} + \max\{r_k, s_k\}} = p_1^{r_1 + s_1} p_2^{r_2 + s_2} \cdots p_k^{r_k + s_k} = \alpha\beta$. ■

Είναι προφανές ότι δύο αριθμοί α και β είναι πρώτοι μεταξύ τους αν και μόνον αν δεν έχουν κοινό πρώτο διαιρέτη. (Ο πρώτος διαιρέτης θα διαιρούσε και τους δύο, άρα και τον μέγιστο κοινό διαιρέτη τους).

Ας δώσουμε και μια άλλη απόδειξη του **πορίσματος 1.23**: Αν α, β, k είναι θετικοί ακέραιοι, τότε ισχύει η ισοδυναμία: $\alpha \mid \beta \Leftrightarrow \alpha^k \mid \beta^k$.
Απόδειξη: Εδώ θα γράψουμε $\alpha = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ και $\beta = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$, όπου $p_1, p_2, \ldots, p_n$ διαφορετικοί πρώτοι και $r_i, s_i \geq 0$, για κάθε $i = 1, 2, \ldots, n$. (Χρησιμοποιούμε το n αντί του k, γιατί το k συμβολίζει εδώ

τον εκθέτη). Έχουμε: $\alpha \mid \beta \Leftrightarrow r_i \leq s_i \Leftrightarrow k(s_i - r_i) \geq 0 \Leftrightarrow kr_i \leq ks_i$ για κάθε $i = 1, 2, \ldots, n$. Σύμφωνα με το λήμμα 1.41 αυτό είναι ισοδύναμο με $\alpha^k = p_1^{kr_1} \cdots p_n^{kr_n} \mid p_1^{ks_1} \cdots p_n^{ks_n} = \beta^k$. ■

Επίσης, μπορούμε να δώσουμε μια «κομψή» απόδειξη του **πορίσματος 1.24**: Αν m θετικός ακέραιος, τότε ο αριθμός $\sqrt[k]{m}$ είναι ρητός αν και μόνον αν το m είναι $k-$στή δύναμη ακεραίου. ($k > 1$.)
Απόδειξη: Έστω $\sqrt[k]{m} = \dfrac{\alpha}{\beta}$ με $\alpha, \beta > 0$ και $(\alpha, \beta) = 1$. $\Big($Η υπόθεση $(\alpha, \beta) = 1$ δεν είναι αυθαίρετη, γιατί $\dfrac{\alpha}{\beta} = \dfrac{\alpha/(\alpha,\beta)}{\beta/(\alpha,\beta)}\Big)$. Υποθέτουμε ότι $\beta > 1$ και p ένας πρώτος διαιρέτης του. Τότε, από τη σχέση $\beta^k m = \alpha^k$ και επειδή προφανώς $p \mid \beta^k$, προκύπτει ότι $p \mid \alpha^k$. Από το πόρισμα 1.35 προκύπτει ότι $p \mid \alpha$. Επομένως $p \mid (\alpha, \beta) = 1$, άτοπο. ■

Πόρισμα 1.44. (i) Αν το $k, m > 1$. Έστω ότι $\sqrt[k]{m} = \lambda \in \mathbb{Z}$. Προφανώς $\lambda > 1$. Αν $\lambda = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$ με $s_i > 0$, για κάθε $i = 1, 2, \ldots, n$ και $p_i \neq p_j$ αν $i \neq j$, είναι η ανάλυση του λ σε γινόμενο πρώτων παραγόντων, τότε $m = p_1^{ks_1} p_2^{ks_2} \cdots p_n^{ks_n}$ είναι η ανάλυση του m σε γινόμενο πρώτων παραγόντων.
(ii) Αν $m = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$, με $r_1, r_2, \ldots, r_n > 0$ και και $p_i \neq p_j$ αν $i \neq j$, είναι η ανάλυση του m σε γινόμενο πρώτων παραγόντων, τότε ο $\sqrt[k]{m}$ είναι ακέραιος αν και μόνον αν $k \mid r_i$, για κάθε $i = 1, 2, \ldots, n$.
Απόδειξη: (i) Προφανώς $\lambda = \sqrt[k]{m} \Leftrightarrow m = \lambda^k = (p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n})^k = p_1^{ks_1} p_2^{ks_2} \cdots p_n^{ks_n}$ είναι η ανάλυση του m σε γινόμενο πρώτων παραγόντων.
(ii) Προκύπτει άμεσα από το (i). Θα μπορούσαμε να κινηθούμε και διαφορετικά. Αν το λ διαιρείτο από κάποιον πρώτο q, διαφορετικό των p_i, τότε $q \mid \lambda^k = m = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$, άτοπο γιατί θα έπρεπε τότε $q = p_i$, για κάποιο i. Επομένως $\lambda = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$, όπου $0 \leq s_i$, για κάθε $i = 1, 2, \ldots, n$. Τώρα $m = \lambda^k \Leftrightarrow p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} = p_1^{ks_1} p_2^{ks_2} \cdots p_n^{ks_n}$ και άρα $ks_i = r_i \Rightarrow k \mid r_i$, για κάθε $i = 1, 2, \ldots, n$. ■

Επίσης, μπορούμε να δώσουμε μια 2^{η} απόδειξη της **άσκησης 1.30**.
Αν $\alpha, \beta, \gamma > 0$, τότε $[(\alpha, \beta), \gamma] = ([\alpha, \gamma], [\beta, \gamma])$ και $([\alpha, \beta], \gamma) = [(\alpha, \gamma), (\beta, \gamma)]$.
Απόδειξη: Προτάσσουμε τους ακόλουθο ισχυρισμό:
Ισχυρισμός: Για κάθε $x, z \in \mathbb{R}$ ισχύουν οι σχέσεις: $\max\{\min\{x, y\}, z\} = \min\{\max\{x, z\}, \max\{y, z\}\}$ και $\min\{\max\{x, y\}, z\} = \max\{\min\{x, z\}, \min\{y, z\}\}$. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $x \geq y$. (Αν $y > x$ επαναλαμβάνουμε συμμετρικά τους συλλογισμούς). Αν λοιπόν $x \geq y$, τότε $\min\{x, y\} = y$ και $\max\{x, y\} = x$. Η πρώτη σχέση γίνεται $\max\{y, z\} = \min\{\max\{x, z\}, \max\{y, z\}\}$ και η δεύτερη σχέση $\min\{x, z\} = \max\{\min\{x, z\}, \min\{y, z\}\}$.
Για την πρώτη σχέση έχουμε: $y \leq x \leq \max\{x, z\}$ και $z \leq \max\{x, z\}$. Επομένως $\max\{y, z\} \leq \max\{x, z\}$ και κατά συνέπεια $\min\{\max\{x, z\}, \max\{y, z\}\} = \max\{y, z\}$. Για τη δεύτερη σχέση έχουμε: $\min\{y, z\} \leq$ $\leq y \leq x$ και $\min\{y, z\} \leq z$. Επομένως $\min\{y, z\} \leq \min\{x, z\}$ και συνεπώς $\max\{\min\{x, z\}, \min\{y, z\}\} =$ $= \min\{x, z\}$. Η απόδειξη του ισχυρισμού είναι πλήρης.
Έστω τώρα $\alpha = p_1^{\kappa_1} p_2^{\kappa_2} \cdots p_n^{\kappa_n}$, $\beta = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$ και $\gamma = p_1^{\mu_1} p_2^{\mu_2} \cdots p_n^{\mu_n}$, όπου $p_1, p_2, \ldots, p_n$ διαφορετικοί πρώτοι και $\kappa_i, \lambda_i, \mu_i \geq 0$, για κάθε $i = 1, 2, \ldots, n$. έχουμε: $[(\alpha, \beta), \gamma] = \Big[\Big(\prod_{i=1}^n p_i^{\kappa_i}, \prod_{i=1}^n p_i^{\lambda_i}\Big), \prod_{i=1}^n p_i^{\mu_i}\Big] =$
$= \Big[\prod_{i=1}^n p_i^{\min\{\kappa_i, \lambda_i\}}, \prod_{i=1}^n p_i^{\mu_i}\Big] = \prod_{i=1}^n p_i^{\max\{\min\{\kappa_i, \lambda_i\}, \mu_i\}} = \prod_{i=1}^n p_i^{\min\{\max\{\kappa_i, \mu_i\}, \max\{\lambda_i, \mu_i\}\}} =$
$= \Big(\prod_{i=1}^n p^{\max\{\kappa_i, \mu_i\}}, \prod_{i=1}^n p^{\max\{\kappa_i, \mu_i\}}\Big) = \Big(\Big[\prod_{i=1}^n p_i^{\kappa_i}, \prod_{i=1}^n p_i^{\mu_i}\Big], \Big[\prod_{i=1}^n p_i^{\lambda_i}, \prod_{i=1}^n p_i^{\mu_i}\Big]\Big) = ([\alpha, \gamma], [\beta, \gamma])$.
Επίσης, $([\alpha, \beta], \gamma) = \Big(\Big[\prod_{i=1}^n p_i^{\kappa_i}, \prod_{i=1}^n p_i^{\lambda_i}\Big], \prod_{i=1}^n p_i^{\mu_i}\Big) = \Big(\prod_{i=1}^n p_i^{\max\{\kappa_i, \lambda_i\}}, \prod_{i=1}^n p_i^{\mu_i}\Big) = \prod_{i=1}^n p_i^{\min\{\max\{\kappa_i, \lambda_i\}, \mu_i\}} =$
$= \prod_{i=1}^n p_i^{\max\{\min\{\kappa_i, \mu_i\}, \min\{\lambda_i, \mu_i\}\}} = \Big[\prod_{i=1}^n p^{\min\{\kappa_i, \mu_i\}}, \prod_{i=1}^n p^{\min\{\kappa_i, \mu_i\}}\Big] = \Big[\Big(\prod_{i=1}^n p_i^{\kappa_i}, \prod_{i=1}^n p_i^{\mu_i}\Big), \Big(\prod_{i=1}^n p_i^{\lambda_i}, \prod_{i=1}^n p_i^{\mu_i}\Big)\Big] =$
$= [(\alpha, \gamma), (\beta, \gamma)]$. ■

Η πρόταση 1.42 γενικεύεται επαγωγικά αν χρησιμοποιήσουμε τους τύπους: $(\alpha_1, \ldots, \alpha_{m-1}, \alpha_m) =$ $= ((\alpha_1, \ldots, \alpha_{m-1}), \alpha_m)$ και $[\alpha_1, \ldots, \alpha_{m-1}, \alpha_m] = [[\alpha_1, \ldots, \alpha_{m-1}], \alpha_m]$.

Κατ' αρχάς, $\min\{\min\{x_1, x_2, \ldots, x_{m-1}\}, x_m\} = \min\{x_1, x_2, \ldots, x_{m-1}, x_m\}$ και
$\max\{\max\{x_1, x_2, \ldots, x_{m-1}\}, x_m\} = \max\{x_1, x_2, \ldots, x_{m-1}, x_m\}$,
για κάθε $x_1, x_2, \ldots, x_{m-1}, x_m \in \mathbb{R}$.

Πρόταση 1.45. Έστω $\alpha_i = p_1^{r_{i1}} p_2^{r_{i2}} \cdots p_k^{r_{ik}}$, όπου $i = 1, 2, \ldots, m$. Τότε έχουμε:
(i) $(\alpha_1, \alpha_2, \ldots, \alpha_m) = p_1^{\min\{r_{11}, r_{21}, \ldots, r_{m1}\}} p_2^{\min\{r_{12}, r_{22}, \ldots, r_{m2}\}} \cdots p_k^{\min\{r_{1k}, r_{2k}, \ldots, r_{mk}\}}$ και
(ii) $[\alpha_1, \alpha_2, \ldots, \alpha_m] = p_1^{\max\{r_{11}, r_{21}, \ldots, r_{m1}\}} p_2^{\max\{r_{12}, r_{22}, \ldots, r_{m2}\}} \cdots p_k^{\max\{r_{1k}, r_{2k}, \ldots, r_{mk}\}}$.
Απόδειξη: (i) Για $m = 2$ είναι η πρόταση 1.42. Έστω $m > 2$. Επειδή $(\alpha_1, \ldots, \alpha_{m-1}, \alpha_m) = ((\alpha_1, \ldots, \alpha_{m-1}), \alpha_m)$, μπορούμε να υποθέσουμε επαγωγικά ότι
$$(\alpha_1, \alpha_2, \ldots, \alpha_{m-1}) = p_1^{\min\{r_{11}, r_{21}, \ldots, r_{m-1,1}\}} p_2^{\min\{r_{12}, r_{22}, \ldots, r_{m-1,2}\}} \cdots p_k^{\min\{r_{1k}, r_{2k}, \ldots, r_{m-1,k}\}}.$$
Επομένως $(\alpha_1, \ldots, \alpha_{m-1}, \alpha_m) = ((\alpha_1, \ldots, \alpha_{m-1}), \alpha_m) = p_1^{\min\{\min\{r_{11}, r_{21}, \ldots, r_{m-1,1}\}, r_{m1}\}} p_2^{\min\{\min\{r_{12}, r_{22}, \ldots, r_{m-1,2}\}, r_{m2}\}}$
$\cdots p_k^{\min\{\min\{r_{1k}, r_{2k}, \ldots, r_{m-1,k}\}, r_{mk}\}} = p_1^{\min\{r_{11}, r_{21}, \ldots, r_{m-1,1}, r_{m1}\}} p_2^{\min\{r_{12}, r_{22}, \ldots, r_{m-1,2}, r_{m2}\}} \cdots p_k^{\min\{r_{1k}, r_{2k}, \ldots, r_{m-1,k}, r_{mk}\}}$.
(ii) Για $m = 2$ είναι η πρόταση 1.42. Έστω $m > 2$. Επειδή $[\alpha_1, \ldots, \alpha_{m-1}, \alpha_m] = [[\alpha_1, \ldots, \alpha_{m-1}], \alpha_m]$, μπορούμε να υποθέσουμε επαγωγικά ότι
$$[\alpha_1, \alpha_2, \ldots, \alpha_{m-1}] = p_1^{\max\{r_{11}, r_{21}, \ldots, r_{m-1,1}\}} p_2^{\max\{r_{12}, r_{22}, \ldots, r_{m-1,2}\}} \cdots p_k^{\max\{r_{1k}, r_{2k}, \ldots, r_{m-1,k}\}}.$$
Επομένως $[\alpha_1, \ldots, \alpha_{m-1}, \alpha_m] = [[\alpha_1, \ldots, \alpha_{m-1}], \alpha_m] = p_1^{\max\{\max\{r_{11}, r_{21}, \ldots, r_{m-1,1}\}, r_{m1}\}} p_2^{\max\{\max\{r_{12}, r_{22}, \ldots, r_{m-1,2}\}, r_{m2}\}}$
$\cdots p_k^{\max\{\max\{r_{1k}, r_{2k}, \ldots, r_{m-1,k}\}, r_{mk}\}} = p_1^{\max\{r_{11}, r_{21}, \ldots, r_{m-1,1}, r_{m1}\}} p_2^{\max\{r_{12}, r_{22}, \ldots, r_{m-1,2}, r_{m2}\}} \cdots p_k^{\max\{r_{1k}, r_{2k}, \ldots, r_{m-1,k}, r_{mk}\}}$. ■

Τίθεται τώρα το ερώτημα: **Υπάρχουν πεπερασμένοι το πλήθος ή άπειροι πρώτοι αριθμοί;**
Υπάρχουν διάφορες αποδείξεις της απειρίας των πρώτων αριθμών. Η απλούστερη είναι του Ευκλείδη.

Θεώρημα 1.46. Υπάρχουν άπειροι πρώτοι αριθμοί.
1η Απόδειξη: (Ευκλείδης) Υποθέτουμε ότι το σύνολο των πρώτων αριθμών είναι πεπερασμένο. Έστω $\{p_1, p_2, \ldots, p_n\}$ το σύνολο των πρώτων αριθμών. Θεωρούμε τον αριθμό $\mathrm{N} = p_1 p_2 \cdots p_n + 1 > 1$. Ο N έχει έναν πρώτο διαιρέτη. Αυτός αναγκαστικά θα πρέπει να είναι κάποιος από τους $p_1, p_2, \ldots, p_n$, έστω ο p_i. Αλλά $p_i \mid p_1 p_2 \cdots p_n$ και $p_i \mid \mathrm{N} = p_1 p_2 \cdots p_n + 1$. Επομένως $p_i \mid \mathrm{N} - p_1 p_2 \cdots p_n = 1$, άτοπο. ■
2η Απόδειξη: Με βάση το (iii) της πρότασης 1.34, αρκεί να βρούμε οσοδήποτε μεγάλο πλήθος ανά δύο πρώτων μεταξύ τους αριθμών. Αυτοί θα έχουν διαφορετικούς πρώτους διαιρέτες. Έστω ένας ακέραιος $n > 1$. Θεωρούμε τους n αριθμούς $n! + 1$, $\frac{n!}{2} + 1$, $\frac{n!}{3} + 1$,..., $\frac{n!}{n-1} + 1$, $(n-1)! + 1$ (κατά φθίνουσα σειρά). Αρκεί να αποδείξουμε ότι οι αριθμοί αυτοί είναι ανά δύο πρώτοι μεταξύ τους. Έστω $1 \le \lambda < \kappa \le n$ και $\delta = \left(\frac{n!}{\lambda} + 1, \frac{n!}{\kappa} + 1\right)$. Τότε $\delta \,\Big|\, \lambda\left(\frac{n!}{\lambda} + 1\right) = n! + \lambda$. Ομοίως $\delta \mid n! + \kappa$. Επομένως $\delta \mid (n! + \kappa) - (n! + \lambda) = \kappa - \lambda$. Επειδή $1 \le \lambda < \kappa \le n$, προκύπτει ότι $1 \le \kappa - \lambda < \kappa \le n$. Άρα το $\kappa - \lambda$ διαιρεί το $\frac{n!}{\kappa} = \frac{1 \cdot 2 \cdots (\kappa - \lambda) \cdots \not{\kappa} \cdots n}{\not{\kappa}}$. Εφόσον $\delta \mid \kappa - \lambda$ και $\kappa - \lambda \,\Big|\, \frac{n!}{\kappa}$, έπεται ότι $\delta \,\Big|\, \frac{n!}{\kappa}$. Αλλά $\delta \,\Big|\, \frac{n!}{\kappa} + 1$, οπότε $\delta \mid 1 \Leftrightarrow \delta = 1$. Επειδή το n μπορεί να πάρει οσοδήποτε μεγάλες τιμές, η απόδειξη θεωρείται πλήρης. ■
3η Απόδειξη: Θέτουμε $n_1 = 2$, $n_2 = n_1 + 1$, $n_3 = n_1 n_2 + 1$, $n_4 = n_1 n_2 n_3 + 1$, ..., $n_k = n_1 n_2 \cdots n_{k-1} + 1$ κ.ο.κ. Θα αποδείξουμε ότι οι αριθμοί $n_1, n_2, n_3, \ldots$ είναι ανά δύο πρώτοι μεταξύ τους. Έστω λοιπόν $1 \le t < k$ και $\delta = (n_t, n_k)$. Επειδή $t < k$, $n_t \mid n_1 n_2 \cdots n_{k-1}$, άρα και $\delta \mid n_1 n_2 \cdots n_{k-1}$. Αλλά $\delta \mid n_k = n_1 n_2 \cdots n_{k-1} + 1$. Επομένως $\delta \mid n_k - n_1 n_2 \cdots n_{k-1} = 1 \Leftrightarrow \delta = 1$. ■
4η Απόδειξη: Θεωρούμε τους **αριθμούς Fermat** $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \ldots$ Είναι προφανές ότι οι αριθμοί αυτοί είναι όλοι περιττοί. Επομένως και οι πρώτοι διαιρέτες τους είναι περιττοί. Αρκεί να αποδείξουμε ότι οι αριθμοί Fermat είναι ανά δύο πρώτοι μεταξύ τους. Έστω $m > n \ge 0$. Με επαγωγή επί του $k = m - n > 0$ μπορούμε να αποδείξουμε ότι $F_n \mid 2^{2^m} - 1$. Έστω $m = n + 1$. Τότε $2^{2^m} - 1 = 2^{2^{n+1}} - 1 = (2^{2^n})^2 - 1 = (2^{2^n} - 1)(2^{2^n} + 1) = (2^{2^n} - 1) F_n$. Υποθέτουμε τώρα ότι $F_n \mid 2^{2^{n+k}} - 1$, για κάποιο θετικό ακέραιο k. Τότε $2^{2^{n+k+1}} - 1 = 2^{2^{n+k} \cdot 2} - 1 = (2^{2^{n+k}})^2 - 1 = (2^{2^{n+k}} + 1)(2^{2^{n+k}} - 1)$ και ο τελευταίος παράγοντας είναι πολλαπλάσιο του F_n, από την επαγωγική υπόθεση. Συμπέρασμα: $F_n \mid 2^{2^m} - 1 = F_m + 2$, όπου $m > n$.

Έστω $\delta = (F_n, F_m)$, όπου $m > n$. Επειδή $\delta \mid F_n$ και $F_n \mid F_m + 2$, έπεται ότι $\delta \mid F_m + 2$. Αλλά $\delta \mid F_m$. Επομένως $\delta \mid 2$. Αλλά ο δ είναι ο μέγιστος κοινός διαιρέτης περιττών, άρα περιττός. Κατά συνέπεια $\delta = 1$.

5η Απόδειξη: Υποθέτουμε ότι το σύνολο των πρώτων είναι πεπερασμένο και $p_1, p_2, \ldots, p_k$ να είναι όλοι οι πρώτοι αριθμοί. Έστω m θετικός ακέραιος. Για κάθε $i \in \{1, 2, \ldots, k\}$ θεωρούμε τον μεγαλύτερο δυνατό μη αρνητικό ακέραιο N_i με την ιδιότητα $p_i^{\mathrm{N}_i} \leq m$. Τότε κάθε θετικός ακέραιος $n \leq m$ γράφεται μονοσήμαντα στη μορφή $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, όπου $0 \leq \alpha_i \leq \mathrm{N}_i$, για κάθε $i = 1, 2, \ldots, k$.

Επομένως $\displaystyle\sum_{n=1}^{m} \frac{1}{n} \leq \sum_{\alpha_1=0}^{\mathrm{N}_1} \sum_{\alpha_2=0}^{\mathrm{N}_2} \cdots \sum_{\alpha_k=0}^{\mathrm{N}_k} \frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = \sum_{\alpha_1=0}^{\mathrm{N}_1} \frac{1}{p_1^{\alpha_1}} \cdot \sum_{\alpha_2=0}^{\mathrm{N}_2} \frac{1}{p_2^{\alpha_2}} \cdots \sum_{\alpha_k=0}^{\mathrm{N}_k} \frac{1}{p_k^{\alpha_k}} = \frac{1 - \frac{1}{p_1^{\mathrm{N}_1+1}}}{1 - \frac{1}{p_1}} \cdot \frac{1 - \frac{1}{p_2^{\mathrm{N}_2+1}}}{1 - \frac{1}{p_2}}$

$\cdots \dfrac{1 - \frac{1}{p_k^{\mathrm{N}_k+1}}}{1 - \frac{1}{p_k}} < \dfrac{1}{1 - \frac{1}{p_1}} \cdot \dfrac{1}{1 - \frac{1}{p_2}} \cdots \dfrac{1}{1 - \frac{1}{p_k}} = \dfrac{p_1}{p_1 - 1} \cdot \dfrac{p_2}{p_2 - 1} \cdots \dfrac{p_k}{p_k - 1}$. Επομένως η σειρά $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n}$ είναι άνω φραγμένη και συνεπώς συγκλίνει. Άτοπο, γιατί $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n} = +\infty$. ■

$\Big($Μια σύντομη απόδειξη του αποτελέσματος $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n} = +\infty$ είναι η ακόλουθη: Υποθέτουμε ότι η σειρά $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n}$ συγκλίνει σ' έναν θετικό πραγματικό αριθμό λ. Τότε $\lambda = \left(1 + \frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6}\right) + \left(\frac{1}{7} + \frac{1}{8}\right) + \cdots >$ $> \left(\frac{1}{2} + \frac{1}{2}\right) + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{6} + \frac{1}{6}\right) + \left(\frac{1}{8} + \frac{1}{8}\right) + \cdots = 1 + \frac{2}{4} + \frac{2}{6} + \frac{2}{8} + \cdots = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots = \lambda$, άτοπο$\Big)$.

Προτού προχωρήσουμε στην 6η απόδειξη της απειρίας των πρώτων αριθμών προτάσσουμε το ακόλουθο λήμμα:

Λήμμα 1.47. Έστω α, m θετικοί ακέραιοι με $m \geq 2$. Τότε υπάρχουν μοναδικοί θετικοί ακέραιοι β, γ τέτοιοι, ώστε $\alpha = \beta\gamma^m$ και επιπλέον το β δεν διαιρείται από τη m-στή δύναμη ακεραίου, παρά μόνον του 1.

Απόδειξη: Έστω γ ο μεγαλύτερος θετικός ακέραιος με $\gamma^m \mid \alpha$. Θέτουμε $\beta = \dfrac{\alpha}{\gamma^m} \Leftrightarrow \alpha = \beta\gamma^m$. Αν το β διαιρείτο από έναν διαιρέτη της μορφής δ^m, τότε $\alpha = \beta'(\delta\gamma)^m$, όπου $\beta' = \dfrac{\beta}{\delta^m}$. Επειδή ο γ είναι ο μεγαλύτερος ακέραιος του οποίου η m-στή δύναμη διαιρεί τον α, θα έχουμε αναγκαστικά $\delta = 1$.

Έστω τώρα ότι $\alpha = \beta_1\gamma_1^m$ και δεν υπάρχει (πλην της μονάδας) m-στή δύναμη ακεραίου που να διαιρεί τον β_1. Τότε θα έχουμε: $\beta\gamma^m = \beta_1\gamma_1^m \Leftrightarrow \beta\left(\dfrac{\gamma}{(\gamma,\gamma_1)}\right)^m = \beta_1\left(\dfrac{\gamma_1}{(\gamma,\gamma_1)}\right)^m$. Αλλά $\left(\dfrac{\gamma}{(\gamma,\gamma_1)}, \dfrac{\gamma_1}{(\gamma,\gamma_1)}\right) = 1$, οπότε και $\left(\left(\dfrac{\gamma}{(\gamma,\gamma_1)}\right)^m, \left(\dfrac{\gamma_1}{(\gamma,\gamma_1)}\right)^m\right) = 1$. Εφόσον $\left(\dfrac{\gamma}{(\gamma,\gamma_1)}\right)^m \Bigg| \beta_1\left(\dfrac{\gamma_1}{(\gamma,\gamma_1)}\right)^m$, από το λήμμα του Ευκλείδη προκύπτει ότι $\left(\dfrac{\gamma}{(\gamma,\gamma_1)}\right)^m \Bigg| \beta_1$ και λόγω της ιδιότητας του β_1, παίρνουμε $\dfrac{\gamma}{(\gamma,\gamma_1)} = 1 \Leftrightarrow \gamma = (\gamma,\gamma_1)$, δηλαδή $\gamma \mid \gamma_1$. Παρόμοια $\gamma_1 \mid \gamma$ και άρα $\gamma = \gamma_1$. Από αυτό προκύπτει ότι και $\beta = \beta_1$. ■

Η περίπτωση $\alpha = 1 = 1 \cdot 1^m$ είναι τετριμμένη. Ας επικεντρωθούμε στην περίπτωση που $\alpha > 1$ και $m = 2$. Έστω $\alpha = p_1^{r_1} p_2^{r_2} p_3^{r_3} \cdots p_k^{r_k}$ η ανάλυση του α σε γινόμενο πρώτων παραγόντων (με $p_i \neq p_j$ για $i \neq j$). Το β του λήμματος κατασκευάζεται ως εξής: Από όλους τους πρώτους p_i διαλέγουμε εκείνους που είναι υψωμένη στην 1η δύναμη. (Αν φυσικά υπάρχουν τέτοιοι). Από τους υπόλοιπους που είναι υψωμένη σε μια δύναμη $r_i \geq 2$ διαλέγουμε εκείνους για τους οποίους ο εκθέτης r_i είναι περιττός. Από κάθε τέτοιο $p_i^{r_i}$ παίρνουμε το p_i και το ενσωματώνουμε στο β, αφήνοντας το $p_i^{r_i-1}$ σε άρτια δύναμη. Έτσι φτιάχνουμε το β. Ό, τι απομείνει είναι γινόμενο πρώτων σε άρτια δύναμη, δηλαδή το γ^2. Για παράδειγμα, έστω ότι $\alpha = 2 \cdot 5^3 \cdot 11^4 \cdot 13^3 \cdot 23^5 \cdot 29$. Τότε $\alpha = (2 \cdot 5 \cdot 13 \cdot 23 \cdot 29)(5 \cdot 11^2 \cdot 13 \cdot 23^2)^2$. Προφανώς $\beta = 2 \cdot 5 \cdot 13 \cdot 23 \cdot 29$ και $\gamma = 5 \cdot 11^2 \cdot 13 \cdot 23^2$. Από τη μοναδικότητα της γραφής $\alpha = \beta\gamma^2$, η μέθοδος αυτή οδηγεί στο σωστό

αποτέλεσμα. Είμαστε τώρα σε θέση να δώσουμε μια 6η απόδειξη της απειρίας των πρώτων αριθμών.

6η Απόδειξη: Έστω $\mathrm{P} = \{p_1, p_2, p_3, \ldots\}$ το σύνολο των πρώτων αριθμών, διατεταγμένων κατ' αύξον μέγεθος. Θα αποδείξουμε ότι $\sum_{p\in\mathrm{P}} \frac{1}{p} = +\infty$, δηλαδή η σειρά των πρώτων απειρίζεται και συνεπώς υπάρχουν άπειροι πρώτοι. Πράγματι, αν $\sum_{p\in\mathrm{P}} \frac{1}{p} < +\infty$, τότε υπάρχει θετικός ακέραιος k τέτοιος, ώστε $\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}$. (Μπορεί το άθροισμα $\sum_{i\geq k+1} \frac{1}{p_i}$ να είναι μηδέν, δηλαδή να μην υπάρχουν πρώτοι p_i με $i \geq k+1$). Αν υπάρχουν, αυτοί λέγονται «μεγάλοι». Οι υπόλοιποι θα λέγονται «μικροί». Έστω N θετικός ακέραιος. Τότε $\sum_{i\geq k+1} \frac{\mathrm{N}}{p_i} < \frac{\mathrm{N}}{2}$. Το πλήθος των ακεραίων από 1 έως N είναι προφανώς N. Τους αριθμούς αυτούς τους χωρίζουμε σε δύο κατηγορίες: Η πρώτη κατηγορία αποτελείται από αυτούς που διαιρούνται μόνον από «μικρούς» πρώτους. Έστω N_s το πλήθος αυτών. Η δεύτερη κατηγορία αποτελείται από αυτούς που διαιρούνται και από «μεγάλους» πρώτους. Έστω N_b το πλήθος αυτών των τελευταίων. Προφανώς $\mathrm{N}_s + \mathrm{N}_b = \mathrm{N}$.
Θα προσπαθήσουμε να βρούμε πρώτα ένα άνω φράγμα για το N_b. Ένας αριθμός μικρότερος ή ίσος του N που διαιρείται με κάποιον από τους μεγάλους πρώτους p_i, $i \geq k+1$ θα είναι της μορφής λp_i. Επειδή $\lambda p_i \leq \mathrm{N}$, θα έχουμε $\lambda \leq \frac{\mathrm{N}}{p_i}$. Επομένως ο αριθμός N_b θα είναι το πολύ $\sum_{i\geq k+1} \frac{\mathrm{N}}{p_i} < \frac{\mathrm{N}}{2}$.
Στη συνέχεια, θα βρούμε ένα άνω φράγμα για το N_s. Ένας αριθμός μικρότερος ή ίσος του N που διαιρείται μόνον από τους πρώτους p_1, p_2, …, p_k θα γράφεται, σύμφωνα με το προηγούμενο λήμμα στη μορφή $\beta\gamma^2$. Επειδή το β δεν διαιρείται από τετράγωνο πρώτου, θα ισούται με 1 ή με γινόμενο διαφορετικών πρώτων παρμένων από το σύνολο $\{p_1, p_2, \ldots, p_k\}$. Τα υποσύνολα του $\{p_1, p_2, \ldots, p_k\}$ είναι 2^k το πλήθος. (Το $\varnothing$ αντιστοιχεί στην περίπτωση $\beta = 1$). Τώρα, $\gamma^2 \leq \beta\gamma^2 \leq \mathrm{N}$. Επομένως $\gamma \leq \sqrt{\mathrm{N}}$. Συνδυάζοντας τα παραπάνω προκύπτει ότι $\mathrm{N}_s \leq 2^k\sqrt{\mathrm{N}}$.
Τελικά λοιπόν $\mathrm{N} = \mathrm{N}_b + \mathrm{N}_s < \frac{\mathrm{N}}{2} + 2^k\sqrt{\mathrm{N}} \Rightarrow \frac{\mathrm{N}}{2} < 2^k\sqrt{\mathrm{N}} \Leftrightarrow \sqrt{\mathrm{N}} < 2^{k+1} \Leftrightarrow \mathrm{N} < 2^{2k+2}$. Επειδή το k, όπως ορίστηκε είναι σταθερό και το N μπορεί να πάρει οσονδήποτε μεγάλες τιμές, καταλήγουμε σε άτοπο. Για παράδειγμα, αν $\mathrm{N} = 2^{2k+2}$, τότε θα είχαμε $2^{2k+2} < 2^{2k+2}$. ■

Άσκηση 35. Δείξτε ότι αν $p_1 < p_2 < p_3 \cdots$ είναι η ακολουθία των πρώτων αριθμών, τότε $p_k \leq 2^{2^{k-1}}$, για κάθε $k = 1, 2, 3, \ldots$
Απόδειξη: Για $k = 1$ έχουμε $p_1 = 2 = 2^{2^0} = 2^{2^{1-1}}$. Έστω $p_k \leq 2^{2^{k-1}}$, για κάθε $k = 1, 2, \ldots, k_0 - 1$. Από την πρώτη απόδειξη της απειρίας των πρώτων αριθμών προκύπτει ότι κάθε πρώτος διαιρέτης του αριθμού $p_1 p_2 \cdots p_{k_0-1} + 1$ είναι διαφορετικός από τους $p_1, p_2, \ldots, p_{k_0-1}$. Επομένως, αν p είναι ένας τέτοιος πρώτος διαιρέτης, τότε $p_{k_0} \leq p \leq p_1 p_2 \cdots p_{k_0-1} + 1$. Αλλά $p_1 p_2 \cdots p_{k_0-1} + 1 \leq 2^{2^0} 2^{2^1} 2^{2^2} \cdots 2^{2^{(k_0-1)-1}} + 1 = 2^{1+2+2^2+\cdots+2^{k_0-2}} + 1 = 2^{2^{k_0-1}-1} + 1 \underset{k_0\geq 1}{\leq} 2^{2^{k_0-1}-1} + 2^{2^{k_0-1}-1} = 2^{2^{k_0-1}}$. ■

Αν ένας περιττός αριθμός είναι σχετικά μεγάλος, πώς μπορούμε να αποφανθούμε αν είναι πρώτος ή σύνθετος; Μια πρώτη σκέψη θα ήταν να δοκιμάσουμε αν διαιρείται με όλους τους πρώτους μέχρι το μισό του. Μια τέτοια διαδικασία είναι μάλλον χρονοβόρα. Η επόμενη πρόταση μειώνει δραματικά το πλήθος των υποψήφιων πρώτων διαιρετών ενός αριθμού.

Πρόταση 1.48. Έστω $m > 2$. Τότε, αν ο m είναι σύνθετος, ο μικρότερος πρώτος που τον διαιρεί είναι το πολύ ίσος με $\lfloor\sqrt{m}\rfloor$.
Απόδειξη: Έστω p ο ελάχιστος πρώτος που διαιρεί τον m. Επειδή ο m είναι σύνθετος, ο αριθμός $n = \frac{m}{p}$ είναι μεγαλύτερος του 1. Άρα ο n έχει έναν πρώτο διαιρέτη q. Ο q είναι προφανώς διαιρέτης του m και συνεπώς $p \leq q$. Μάλιστα $pq \mid m$ και κατά συνέπεια $pq \leq m$. Αλλά $p^2 \leq pq \leq m$. Επομένως $p \leq \sqrt{m}$. Επειδή ο $\lfloor\sqrt{m}\rfloor$ είναι ο μέγιστος ακέραιος που δεν υπερβαίνει τον m, θα έχουμε $p \leq \lfloor\sqrt{m}\rfloor$. ■

Για παράδειγμα, ο αριθμός 439 είναι πρώτος, ενώ ο 437 είναι σύνθετος. Παρατηρούμε ότι $20^2 = 400$

και $21^2 = 441$. Επομένως $\lfloor\sqrt{439}\rfloor = \lfloor\sqrt{437}\rfloor = 20$. Επομένως αρκεί να ελέγξουμε αν οι αριθμοί αυτοί διαιρούνται με κάποιον από τους πρώτους 2, 3, 5, 7, 11, 13, 17 και 19. Επειδή και οι δύο είναι περιττοί, ο 2 αποκλείεται. Τα πολλαπλάσια του 5 λήγουν σε 0 ή 5. Άρα και ο 5 αποκλείεται. Πράγματι, $439 = 5\cdot 87+4$. Αν και γνωρίζουμε το γνωστό κριτήριο για το 3, ας διαιρέσουμε το 439 με το 3. $439 = 3\cdot 146+1$. Επίσης, $439 = 7\cdot 62+5$, $439 = 11\cdot 39+10$, $439 = 13\cdot 33+10$, $439 = 17\cdot 25+14$ και τέλος $439 = 19\cdot 23+2$. Άρα ο 439 είναι πρώτος.
Τώρα, $437 = 3\cdot 145+2$, $437 = 5\cdot 87+2$, $437 = 7\cdot 62+3$, $437 = 11\cdot 39+8$, $437 = 13\cdot 33+8$, $437 = 17\cdot 25+12$. Τέλος όμως $437 = 19\cdot 23$. Επομένως ο $437 = 19\cdot 23$ είναι σύνθετος.

Άσκηση 36. Υπάρχουν άπειροι πρώτοι της μορφής $4\lambda+3$.
Απόδειξη: Οι περιττοί πρώτοι είναι της μορφής $4\lambda+1$ ή $4\lambda+3$. (Φυσικά ο μοναδικός άρτιος πρώτος, το 2 είναι της μορφής $4\lambda+2$ με $\lambda=0$). Υποθέτουμε ότι το σύνολο των πρώτων της μορφής $4\lambda+3$ είναι πεπερασμένο. Έστω $4\lambda_1+3$, $4\lambda_2+3$,..., $4\lambda_n+3$ όλοι αυτοί οι πρώτοι. Σχηματίζουμε τον αριθμό $\mathrm{M} = 4(4\lambda_1+3)(4\lambda_2+3)\cdots(4\lambda_n+3)-1$. Ο αριθμός M είναι προφανώς περιττός. Άρα όλοι οι πρώτοι διαιρέτες του είναι περιττοί, δηλαδή της μορφής $4\lambda+1$ ή $4\lambda+3$. Παρατηρούμε ότι δύο αριθμοί της μορφής $4\lambda+1$, όταν πολλαπλασιαστούν δίνουν γινόμενο της ιδίας μορφής. Πράγματι, $(4\lambda+1)(4\lambda'+1) = 4(4\lambda\lambda'+\lambda+\lambda')+1$. Κατά συνέπεια δεν μπορεί όλοι οι πρώτοι διαιρέτες του M να είναι της μορφής $4\lambda+1$, γιατί ο M είναι της μορφής $4\lambda+3$. Πράγματι, αν $\mu = (4\lambda_1+3)(4\lambda_2+3)\cdots(4\lambda_n+3)$, τότε $\mathrm{M} = 4\mu-1 = 4(\mu-1)+3$. Επομένως κάποιος πρώτος διαιρέτης p του M είναι της μορφής $p = 4\lambda+3$, δηλαδή ο p είναι κάποιος από τους $4\lambda_1+3$, $4\lambda_2+3$,..., $4\lambda_n+3$. Τότε όμως $p \mid 4(4\lambda_1+3)(4\lambda_2+3)\cdots(4\lambda_n+3)$ και επειδή $p \mid \mathrm{M}$, θα πρέπει $p \mid -1$, άτοπο. ■

Θεώρημα 1.49. (Legendre) Έστω $n \geq 2$ ακέραιος και p πρώτος. Τότε ο εκθέτης $\alpha(p)$ του p στην ανάλυση του $n!$ σε γινόμενο πρώτων παραγόντων ισούται με $\alpha(p) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$.

Απόδειξη: Κατ' αρχάς παρατηρούμε ότι το άθροισμα $\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$ είναι στην πραγματικότητα πεπερασμένο, αφού για αρκούντως μεγάλο i θα έχουμε $\frac{n}{p^i} < 1$ και επομένως $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$. Αρχικά μετράμε τα πολλαπλάσια του p που είναι μικρότερα ή ίσα του n. Κάθε ένα από αυτά συνεισφέρει από μία μονάδα στον εκθέτη του p. Αν λοιπόν $kp \leq n$, τότε $k \leq \frac{n}{p}$. Ο μέγιστος τέτοιος k είναι προφανώς ίσος με $\left\lfloor \frac{n}{p} \right\rfloor$. Αλλά από αυτά τα πολλαπλάσια του p ενδεχομένως υπάρχουν κάποια που διαιρούνται με το p^2 και αυτά συνεισφέρουν ακόμη μία μονάδα το καθένα στον εκθέτη του p. Το πλήθος τους υπολογίζεται ανάλογα και βρίσκεται ίσο με $\left\lfloor \frac{n}{p^2} \right\rfloor$. Επίσης, από τα προηγούμενα υπάρχουν κάποια που διαιρούνται με το p^3 και το καθένα συνεισφέρει ακόμη μία μονάδα στον εκθέτη του p. Αυτά είναι $\left\lfloor \frac{n}{p^3} \right\rfloor$ το πλήθος. Προχωρώντας κατ' αυτόν τον τρόπο συνάγουμε το επιθυμητό συμπέρασμα.
Αν θέλουμε να είμαστε πιο αυστηροί στην απόδειξη (δεν ξέρω αν χρειάζεται) θα προχωρήσουμε ως εξής: Έστω $\mathrm{A}_i \subseteq \{1,2,\ldots,n\}$ το σύνολο των αριθμών που διαιρούνται με το p^i. Προφανώς $\mathrm{A}_1 \supseteq \mathrm{A}_2 \supseteq \mathrm{A}_3 \supseteq \cdots$. Θέτουμε $\mathrm{B}_i = \mathrm{A}_i \setminus \mathrm{A}_{i+1}$, για κάθε $i = 1,2,3,\ldots$ Το B_i αποτελείται από εκείνους τους αριθμούς από το σύνολο $\{1,2,\ldots,n\}$, οι οποίοι διαιρούνται ακριβώς από το p^i και όχι από μεγαλύτερη δύναμη του p. Προφανώς $|\mathrm{A}_i| = \left\lfloor \frac{n}{p^i} \right\rfloor$. Επομένως $|\mathrm{B}_i| = |\mathrm{A}_i| - |\mathrm{A}_{i+1}| = \left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor$. Επειδή ο εκθέτης του p στην ανάλυση κάθε αριθμού του B_i είναι ακριβώς i, συμπεραίνουμε ότι το γινόμενο των στοιχείων του B_i θα μας δώσει τον p υψωμένο στην $i\cdot|\mathrm{B}_i|$. Επομένως ο συνολικός εκθέτης του p στο $n!$ θα ισούται με $\sum_{i=1}^{\infty} i|\mathrm{B}_i| = \sum_{i=1}^{\infty} i\cdot\left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor\right) = \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor + 2\cdot\left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor\right) + 3\cdot\left(\left\lfloor \frac{n}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^4} \right\rfloor\right) + \cdots =$
$= \left\lfloor \frac{n}{p} \right\rfloor - \cancel{\left\lfloor \frac{n}{p^2} \right\rfloor} + 2\left\lfloor \frac{n}{p^2} \right\rfloor - 2\cancel{\left\lfloor \frac{n}{p^3} \right\rfloor} + 3\left\lfloor \frac{n}{p^3} \right\rfloor - 3\cancel{\left\lfloor \frac{n}{p^4} \right\rfloor} + 4\left\lfloor \frac{n}{p^4} \right\rfloor - 4\cancel{\left\lfloor \frac{n}{p^5} \right\rfloor} + \cdots = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \left\lfloor \frac{n}{p^4} \right\rfloor + \cdots$ ■

Για παράδειγμα, αν $n = 7$, τότε η μέγιστη δύναμη του 3 που διαιρεί το $7! = 5040$ είναι 3^α, όπου $\alpha = \left\lfloor \frac{7}{3} \right\rfloor + \left\lfloor \frac{7}{3^2} \right\rfloor + \cdots = \left\lfloor \frac{7}{3} \right\rfloor = 2$. Η μέγιστη δύναμη του 2 που διαιρεί το 7! είναι $2^{\lfloor 7/2\rfloor + \lfloor 7/4\rfloor} = 2^{3+1} = 2^4$.

Η μέγιστη δύναμη του 11 που διαιρεί το 7! είναι $11^{\lfloor 7/11 \rfloor} = 11^0 = 1$, όπως αναμενόταν.

Το παραπάνω θεώρημα μας επιτρέπει να δώσουμε μια άλλη απόδειξη ότι ο διωνυμικός συντελεστής $\binom{n}{k}$ είναι ακέραιος, δηλαδή ότι το $k!$ διαιρεί το γινόμενο k διαδοχικών ακεραίων $n(n-1)\cdots(n-k+1)$. (Βλέπε **άσκηση 1.12**).

Απόδειξη: Έχουμε $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$. Έστω p πρώτος. Γνωρίζουμε ότι ο εκθέτης του p στην ανάλυση του $n!$ σε γινόμενο πρώτων ισούται με $\sum_{i=1}^{\infty} \left\lfloor \dfrac{n}{p^i} \right\rfloor$. Ανάλογα, οι εκθέτες του p στην ανάλυση των $k!$ και $(n-k)!$ σε γινόμενα πρώτων είναι ίσοι με $\sum_{i=1}^{\infty} \left\lfloor \dfrac{k}{p^i} \right\rfloor$ και $\sum_{i=1}^{\infty} \left\lfloor \dfrac{n-k}{p^i} \right\rfloor$ αντίστοιχα. Συμπεραίνουμε λοιπόν ότι ο εκθέτης του p στην ανάλυση του $k!(n-k)!$ σε γινόμενο πρώτων ισούται με $\sum_{i=1}^{\infty} \left(\left\lfloor \dfrac{k}{p^i} \right\rfloor + \left\lfloor \dfrac{n-k}{p^i} \right\rfloor \right)$. Αλλά ξέρουμε ότι $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor$, για κάθε $x, y \in \mathbb{R}$. Επομένως $\sum_{i=1}^{\infty} \left(\left\lfloor \dfrac{k}{p^i} \right\rfloor + \left\lfloor \dfrac{n-k}{p^i} \right\rfloor \right) \leq \sum_{i=1}^{\infty} \left\lfloor \dfrac{k+n-k}{p^i} \right\rfloor = \sum_{i=1}^{\infty} \left\lfloor \dfrac{n}{p^i} \right\rfloor$. ■

Πρόταση 1.50. Αν n είναι θετικός ακέραιος, τότε υπάρχουν n διαδοχικοί σύνθετοι αριθμοί.
Απόδειξη: Θεωρούμε τους n διαδοχικούς αριθμούς: $(n+1)!+2$, $(n+1)!+3$,...,$(n+1)!+(n+1)$. Κάθε αριθμός από τους παραπάνω είναι της μορφής $(n+1)!+k$, όπου $2 \leq k \leq n+1$. Άρα το k διαιρεί το $(n+1)!$ και συνεπώς το $(n+1)!+k$. ■

Με βάση την παραπάνω πρόταση συμπεραίνουμε ότι υπάρχουν **οσοδήποτε μεγάλα διαστήματα** μεταξύ των θετικών ακεραίων **στα οποία δεν υπάρχει κανένας πρώτος αριθμός**. Από την άλλη μεριά, έχουν παρατηρηθεί ζεύγη πρώτων αριθμών που διαφέρουν κατά 2. Τέτοια ζεύγη είναι $(3,5)$, $(11,13)$, $(17,19)$, αλλά και πολύ μεγάλα, όπως $(1000037, 1000039)$. Αυτοί οι πρώτοι της μορφής p, $p+2$ ονομάζονται **δίδυμοι πρώτοι**. Δεν έχει ακόμη αποδειχθεί αν υπάρχουν άπειρα ζεύγη διδύμων πρώτων. Φαίνεται ότι οι πρώτοι αριθμοί κατανέμονται στην ακολουθία των θετικών ακεραίων, θα λέγαμε κατά τρόπο «ακανόνιστο».

Αν με $\pi(x)$ συμβολίσουμε το πλήθος των πρώτων που είναι μικρότεροι ή ίσοι του $x \geq 0$, τότε ισχύει το εξής περίφημο:

Θεώρημα 1.51. (Θεώρημα των Πρώτων Αριθμών) Η συνάρτηση $\pi(x)$ προσεγγίζεται ασυμπτωτικά από τη συνάρτηση $f(x) = \dfrac{x}{\log x}$, δηλαδή

$$\lim_{x \to +\infty} \frac{\pi(x) \log x}{x} = 1,$$

όπου με $\log x$ συμβολίζουμε τον φυσικό λογάριθμο του x. ■

Το Θεώρημα των πρώτων αριθμών απέδειξαν, ανεξάρτητα ο ένας από τον άλλο το 1896 οι Charles Jean de la Vallée-Poussin και Jacques Hadamard με χρήση της Θεωρίας των Μιγαδικών Συναρτήσεων και πιο συγκεκριμένα, χρησιμοποιώντας τη συνάρτηση Ζήτα του Bernhard Riemann.
Το 1948 οι Atle Selberg και Paul Erdős, πάλι ανεξάρτητα ο ένας απ' τον άλλο, έδωσαν πιο στοιχειώδεις αποδείξεις αποφεύγοντας τη χρήση μιγαδικών συναρτήσεων. Και στις δύο αποδείξεις όμως χρησιμοποιείται ο ίδιος ασυμπτωτικός τύπος τον οποίο είχε ανακαλύψει ο Atle Selberg λίγους μήνες νωρίτερα.
Ένα άλλο σημαντικό θεώρημα το οποίο περιγράφει την κατανομή των πρώτων αριθμών είναι το **αίτημα του Bertrand:**

Θεώρημα 1.52. (Αίτημα του Bertrand) Αν $n > 1$, τότε υπάρχει πρώτος p τέτοιος, ώστε

$$n < p < 2n.$$

■

Στην παράγραφο 1.6 δίνουμε μια απόδειξη του αιτήματος αυτού. Επομένως το «αίτημα» (postulate) του

Bertrand δεν είναι αίτημα, δηλαδή αξίωμα, αλλά θεώρημα. Ο πρώτος που έδωσε μια απόδειξη του θεωρήματος αυτού ήταν ο Ρώσος μαθηματικός Pafnuty Lvovich Chebyshev.

Πόρισμα 1.53. Με την υπόθεση ότι ισχύει το αίτημα του Bertrand προκύπτει η σχέση $p_k \leq 2^k$, όπου p_k ο k-στός πρώτος. Ιδιαιτέρως $p_k < 2^k$, για κάθε $k > 1$.
Απόδειξη: $p_1 = 2 = 2^1$. Θα δείξουμε ότι $p_k < 2^k$, για κάθε $k > 1$. Πράγματι, $p_2 = 3 < 2^2$. Έστω $p_k < 2^k$, για κάποιον θετικό ακέραιο $k \geq 2$. Σύμφωνα με το αίτημα του Bertrand υπάρχει πρώτος p τέτοιος, ώστε $p_k < p < 2p_k$. Επειδή $p_k < p$, θα πρέπει $p_{k+1} \leq p < 2p_k \leq 2 \cdot 2^k = 2^{k+1}$. ■

ΛΥΜΕΝΕΣ ΑΣΚΗΣΕΙΣ

Άσκηση 37. Βρείτε τον μέγιστο κοινό διαιρέτη και το ελάχιστο κοινό πολλαπλάσιο των αριθμών $\alpha = 2^3 \cdot 3^2 \cdot 11^4 \cdot 37^3$ και $\beta = 2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 29 \cdot 37^4$.
Λύση: $\alpha = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^4 \cdot 29^0 \cdot 37^3$ και $\beta = 2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 29 \cdot 37^4$. Επομένως $(\alpha, \beta) = 2^{\min\{3,2\}} \cdot 3^{\min\{2,1\}} \cdot 5^{\min\{0,2\}} \cdot 7^{\min\{0,1\}} \cdot 11^{\min\{4,1\}} \cdot 29^{\min\{0,1\}} \cdot 37^{\min\{3,4\}} = 2^2 \cdot 3 \cdot 11 \cdot 37^3 = 6686196$. Επίσης $[\alpha, \beta] = 2^{\max\{3,2\}} \cdot 3^{\max\{2,1\}} \cdot 5^{\max\{0,2\}} \cdot 7^{\max\{0,1\}} \cdot 11^{\max\{4,1\}} \cdot 29^{\max\{0,1\}} \cdot 37^{\max\{3,4\}} = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11^4 \cdot 29 \cdot 37^4 = 10026426624845400$. ■

Η παραπάνω διαδικασία ακολούθησε τον τυπικό κανόνα της πρότασης 1.42. «Με το μάτι», για τον μέγιστο κοινό διαιρέτη παίρνουμε **μόνον τους κοινούς πρώτους στη μικρότερη δύναμη**: $(\alpha, \beta) = 2^2 \cdot 3 \cdot 11 \cdot 37^3$. Για το ελάχιστο κοινό πολλαπλάσιο τους παίρνουμε **όλους (κοινούς και μη κοινούς) στη μεγαλύτερη δύναμη**: $[\alpha, \beta] = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11^4 \cdot 29 \cdot 37^4$.

Άσκηση 38. Ποιοι από τους ακόλουθους αριθμούς είναι πρώτοι και ποιοι σύνθετοι;

373, 457, 511, 619, 629, 701.

Λύση: Εφαρμόζουμε την πρόταση 1.48. $\sqrt{373} = 19,31\ldots$ Άρα $\lfloor\sqrt{373}\rfloor = 19$. Υποψήφιοι πρώτοι διαιρέτες: 3, 5, 7, 11, 13, 17, 19. Έχουμε: $373 = 3 \cdot 124 + 1$, $373 = 5 \cdot 74 + 3$, $373 = 7 \cdot 53 + 2$, $373 = 11 \cdot 33 + 10$, $373 = 13 \cdot 28 + 9$, $373 = 17 \cdot 21 + 16$, $373 = 19 \cdot 19 + 12$. Άρα ο 373 είναι πρώτος.
$\sqrt{457} = 21,37\ldots$ Άρα $\lfloor\sqrt{457}\rfloor = 21$. Υποψήφιοι πρώτοι διαιρέτες: 3, 5, 7, 11, 13, 17, 19. Έχουμε: $457 = 3 \cdot 152 + 1$, $457 = 5 \cdot 91 + 2$, $457 = 7 \cdot 65 + 2$, $457 = 11 \cdot 41 + 6$, $457 = 13 \cdot 35 + 2$, $457 = 17 \cdot 26 + 15$, $457 = 19 \cdot 24 + 1$. Άρα ο 457 είναι πρώτος.
$\sqrt{511} = 22,605\ldots$ Άρα $\lfloor\sqrt{511}\rfloor = 22$. Υποψήφιοι πρώτοι διαιρέτες: 3, 5, 7, 11, 13, 17, 19. Έχουμε: $511 = 3 \cdot 170 + 1$, $511 = 5 \cdot 102 + 1$, $511 = 7 \cdot 73$. Άρα ο 511 είναι σύνθετος.
$\sqrt{619} = 24,87\ldots$ Άρα $\lfloor\sqrt{619}\rfloor = 24$. Υποψήφιοι πρώτοι διαιρέτες: 3, 5, 7, 11, 13, 17, 19, 23. Έχουμε: $619 = 3 \cdot 206 + 1$, $619 = 5 \cdot 123 + 4$, $619 = 7 \cdot 88 + 3$, $619 = 11 \cdot 56 + 3$, $619 = 13 \cdot 47 + 8$, $619 = 17 \cdot 36 + 7$, $619 = 19 \cdot 32 + 11$, $619 = 23 \cdot 26 + 21$. Άρα ο 619 είναι πρώτος.
$\sqrt{629} = 25,07\ldots$ Άρα $\lfloor\sqrt{629}\rfloor = 25$. Υποψήφιοι πρώτοι διαιρέτες: 3, 5, 7, 11, 13, 17, 19, 23. Έχουμε: $629 = 3 \cdot 209 + 2$, $629 = 5 \cdot 125 + 4$, $629 = 7 \cdot 89 + 6$, $629 = 11 \cdot 57 + 2$, $629 = 13 \cdot 48 + 5$, $629 = 17 \cdot 37$. Άρα ο 629 είναι σύνθετος.
$\sqrt{701} = 26,47\ldots$ Άρα $\lfloor\sqrt{701}\rfloor = 26$. Υποψήφιοι πρώτοι διαιρέτες: 3, 5, 7, 11, 13, 17, 19, 23. Έχουμε: $701 = 3 \cdot 233 + 2$, $701 = 5 \cdot 140 + 1$, $701 = 7 \cdot 100 + 1$, $701 = 11 \cdot 63 + 8$, $701 = 13 \cdot 53 + 12$, $701 = 17 \cdot 41 + 4$, $701 = 19 \cdot 36 + 17$, $701 = 23 \cdot 30 + 11$. Άρα ο 701 είναι πρώτος. ■

Άσκηση 39. Δείξτε ότι αν α, β είναι θετικοί ακέραιοι και $\alpha^3 \mid \beta^2$, τότε $\alpha \mid \beta$. Ισχύει το ίδιο συμπέρασμα αν $\alpha^2 \mid \beta^3$;
Απόδειξη: Αν $\alpha = 1$, τότε προφανώς $\alpha^3 \mid \beta$. Έστω $\alpha > 1$ και $\alpha = p_1^{r_1} \cdots p_k^{r_k}$ είναι η ανάλυση του α σε γινόμενο πρώτων παραγόντων, με $k \geq 1$, $r_i > 0$ για κάθε $i = 1, \ldots, k$ και $p_i \neq p_j$ για $i \neq j$. Για κάθε $i = 1, 2 \ldots, k$ ο $p_i^{3r_i}$ διαιρεί τον β^2, άρα και ο p_i διαιρεί τον β^2, άρα και τον β. Έστω $p_i^{s_i}$ η μεγαλύτερη δύναμη του p_i που διαιρεί τον β. Εφόσον $\alpha^3 \mid \beta^2$, θα έχουμε $3r_i \leq 2s_i \Leftrightarrow r_i \leq \frac{2}{3}s_i < s_i$. Σύμφωνα με το λήμμα 41, $\alpha \mid \beta$. Αν τώρα $\alpha^2 \mid \beta^3$, τότε ο α δεν διαιρεί αναγκαστικά τον β. Για παράδειγμα, αν $\alpha = 32$ και $\beta = 16$, τότε $\alpha^2 = (2^5)^2 = 2^{10}$ και $\beta^3 = (2^4)^3 = 2^{12}$, δηλαδή $\alpha^2 \mid \beta^3$, ενώ $\alpha = 32 \nmid 16 = \beta$. ■

Άσκηση 40. Οι αριθμοί p, $p+2$ και $p+4$ είναι πρώτοι. Να βρεθούν οι αριθμοί αυτοί.
Λύση: Κατ' αρχάς, για κάθε ακέραιο n κάποιος από τους n, $n+2$ και $n+4$ διαιρείται από το 3. Αν $3 \nmid n$, τότε $n = 3k+1$ ή $n = 3k+2$. Στην πρώτη περίπτωση $n+2 = 3(k+1)$, ενώ στη δεύτερη $n+4 = 3(k+2)$. Σε κάθε περίπτωση κάποιος από τους n, $n+2$ και $n+4$ διαιρείται από το 3. Στην περίπτωσή μας, επειδή οι αριθμοί είναι πρώτοι, αυτός που διαιρείται με το 3 θα είναι ο 3. Επειδή $p+2, p+4 \geq 4$ ο p ισούται με 3. Άρα $p+2 = 5$ και $p+4 = 7$. ■

Άσκηση 41. **(i)** Αν α θετικός ακέραιος και p πρώτος, με $\alpha^2 - p = 9$, να βρεθούν οι α και p.
(ii) Αν ο $17p+1$ είναι τέλειο τετράγωνο, όπου p πρώτος, να βρεθεί ο p.
Λύση: **(i)** $\alpha^2 - p = 9 \Leftrightarrow p = \alpha^2 - 9 = (\alpha-3)(\alpha+3)$. Επειδή ο p είναι πρώτος, πρέπει $\alpha - 3 = 1 \Leftrightarrow \alpha = 4$. Επομένως $p = 4+3 = 7$.
(ii) Έστω $17p+1 = m^2 \Leftrightarrow 17p = m^2-1 = (m-1)(m+1)$. Επειδή $p \geq 2$, $17p+1 \geq 35 > 25 = 5^2$. Επομένως $m > 5$ και κατά συνέπεια $m-1 \geq 5$. Επειδή $17p = (m-1)(m+1)$ και οι 17 και p είναι πρώτοι, θα έχουμε $17 = m-1$ και $p = m+1 = 17+2 = 19$, λύση αποδεκτή, ή $17 = m+1$ και $p = m-1 = 17-2 = 15$, άτοπο γιατί ο 15 δεν είναι πρώτος. Άρα $p = 19$. ■

Άσκηση 42. Έστω p και $p+2$ πρώτοι με $3 < p$. (Πχ. $p = 5$ και $p+2 = 7$ ή $p = 11$ και $p+2 = 13$). Τότε το άθροισμά τους $2p+2$ διαιρείται με το 12.
Απόδειξη: Εφόσον $p > 3$, τότε το p είναι της μορφής $p = 3k+1$ ή $p = 3k+2$. Αν $p = 3k+1$, τότε $p+2 = 3k+3 = 3(k+1)$, δηλαδή $3 \mid p+2 > 3$, άτοπο γιατί $p+2$ πρώτος. Άρα $p = 3k+2$, οπότε $p+2 = 3k+4$. Επομένως $2p+2 = 6k+6 = 6(k+1)$. Άρα $6 \mid 2p+2$ και συνεπώς και $3 \mid 2p+2$. Επίσης, εφόσον το p είναι πρώτος μεγαλύτερος του 3, τότε $p \geq 5$ και άρα το p θα είναι της μορφής $4k+1$ ή $4k+3$. (Η περίπτωση $p = 4k+2$ μας δίνει άρτιο). Έστω $p = 4k+1$. Τότε $p+2 = 4k+3$. Επομένως $2p+2 = p+(p+2) = 8k+4 = 4(2k+1)$, ήτοι $4 \mid 2p+2$. Αν $p = 4k+3$, τότε $p+2 = 4k+5$. Επομένως $2p+2 = p+(p+2) = 8k+8 = 8(k+1)$, ήτοι $8 \mid 2p+2$ και συνεπώς $4 \mid 2p+2$. Σε κάθε περίπτωση έχουμε $4 \mid 2p+2$. Επειδή, όπως δείξαμε $3 \mid 2p+2$ και επειδή $(3,4) = 1$, έπεται $3 \cdot 4 = 12 \mid 2p+2$. ■

Άσκηση 43. Το άθροισμα δύο θετικών αριθμών είναι 5432 και το ελάχιστο κοινό πολλαπλάσιό τους 223020. Βρείτε τους αριθμούς αυτούς.
Λύση: Έστω x, y οι αριθμοί αυτοί. Παρατηρούμε ότι $5432 = 2^3 \cdot 7 \cdot 97$ και $223020 = 2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 59$. Επειδή $7 \mid [x,y]$, κάποιος από αυτούς διαιρείται από το 7. Αν ο άλλος δεν διαιρείτο από το 7, τότε $7 \nmid x+y$, άτοπο. Επίσης κάποιος διαιρείται από το $2^2 = 4$. Αν ο άλλος δεν διαιρείτο από το 4, τότε $4 \nmid x+y$, άτοπο. Άρα και οι δύο διαιρούνται από το $4 \cdot 7 = 28$. Έστω $x_1 = \dfrac{x}{28}$ και $y_1 = \dfrac{y}{28}$. Τότε $x_1 + y_1 = \dfrac{5432}{28} = 2 \cdot 97 = 194$ και $[x_1, y_1] = \dfrac{223020}{28} = 3^3 \cdot 5 \cdot 59$. Επειδή κανείς από τους πρώτους που διαιρούν το $[x_1, y_1]$ δεν διαιρεί το $x_1 + y_1$, ένας μόνον διαιρείται από το $3^3 = 27$, ένας μόνον από το 5 και ένας μόνον από το 59. Επειδή $27 \cdot 59 > 5 \cdot 59 = 295 > 194$, αυτός που διαιρείται από το 59 πρέπει να είναι ο 59. Ο άλλος θα είναι ο $194 - 59 = 135 = 27 \cdot 5$. Αν $x_1 = 135$ και $y_1 = 59$, τότε $x = 28 \cdot 135 = 3780$ και $y = 28 \cdot 59 = 1652$.
Η άσκηση αυτή θα μπορούσε να λυθεί και διαφορετικά. Πρώτα λύνουμε ξανά την άσκηση 33 στη σελίδα 28, χρησιμοποιώντας πρώτους αριθμούς. Θα δείξουμε ότι $(x,y) = (x+y, [x,y])$. Έστω $\delta = (x,y)$. Τότε $x = \delta x'$ και $y = \delta y'$ με $(x', y') = 1$. Επίσης, $\delta = (x,y) = (x+y, [x,y]) \Leftrightarrow 1 = \left(\dfrac{x+y}{\delta}, \dfrac{[x,y]}{\delta}\right) = (x'+y', [x',y']) = (x'+y', x'y')$. Αρκεί να δείξουμε ότι $(x'+y', x'y') = 1$. Αν ο $(x'+y', x'y')$ ήταν μεγαλύτερος της μονάδας, τότε θα είχε έναν πρώτο διαιρέτη p. Εφόσον $p \mid x'y'$, ο p θα διαιρούσε κάποιον από τους x', y'. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $p \mid x'$. Επειδή όμως $p \mid x'+y'$, ο p θα διαιρούσε και τον y', άτοπο γιατί $(x', y') = 1$. Επομένως $(x'+y', x'y') = 1$ και τελειώσαμε.
Τώρα, εφόσον $x+y = 5432$ και $[x,y] = 223020$, έχουμε $(x,y) = (x+y, [x,y]) = (5432, 223020) = (2^3 \cdot 7 \cdot 97, 2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 59) = 2^2 \cdot 7 = 28$. Επομένως $xy = (x,y)[x,y] = 28 \cdot 223020 = 6244560 = 2^4 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 59$. Επομένως οι x, y είναι οι ρίζες της δευτεροβάθμιας εξίσωσης $t^2 - 5432t + 6244560 = 0$. Η διακρίνουσα του τριωνύμου είναι $\Delta = 2^6 \cdot 7^2 \cdot 97^2 - 2^6 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 59 = 2^6 \cdot 7^2 \cdot (97^2 - 3^3 \cdot 5 \cdot 59) = 2^6 \cdot 7^2 (9409 - 7965) = 2^6 \cdot 7^2 \cdot 1444 = 2^6 \cdot 7^2 \cdot 2^2 \cdot 19^2 = 2^8 \cdot 7^2 \cdot 19^2 = (2^4 \cdot 7 \cdot 19)^2 = 2128^2$. Επομένως $t = \dfrac{5432 \pm 2128}{2} =$

$$= 2716 \pm 1064 = \begin{cases} 2716 + 1064 = 3780 \text{ ή} \\ 2716 - 1064 = 1652 \end{cases}$$ ■

Άσκηση 44. Δείξτε ότι αν ο θετικός ακέραιος $n > 4$ είναι σύνθετος, τότε $n \mid (n-1)!$
Απόδειξη: Εφόσον ο n είναι σύνθετος, υπάρχει γνήσιος διαιρέτης του m, με $1 < m < n$. Διακρίνουμε δύο περιπτώσεις: 1) $\frac{n}{m} = m \Leftrightarrow n = m^2$. Επειδή $n > 4$, έπεται ότι $m > 2$. Επομένως $2m < m^2 = n$. Οι αριθμοί m και $2m$ είναι μικρότεροι του n και συνεπώς το γινόμενό τους $m \cdot 2m = 2m^2 = 2n$ διαιρεί το $(n-1)!$ Άρα και το n διαιρεί το $(n-1)!$. 2) $\frac{n}{m} \neq m$. Τότε οι m και $\frac{n}{m}$ είναι διαφορετικοί και προφανώς μικρότεροι του n, οπότε το γινόμενό τους $m \cdot \frac{n}{m} = n$ διαιρεί το $(n-1)!$ ■

Άσκηση 45. (i) Πόσα μηδενικά έχει στο τέλος ο αριθμός $83!$;
(ii) Για ποιες τιμές του $n > 0$ ο αριθμός $n!$ τελειώνει σε ακριβώς 26 μηδενικά;
(iii) Είναι δυνατόν το $n!$ να τελειώνει σε ακριβώς 36 μηδενικά;
Λύση: (i) Εφαρμόζουμε το θεώρημα του Legendre (Θεώρημα 1.49). Το πλήθος των μηδενικών στο τέλος του $n!$ ισούται με τη μεγαλύτερη δύναμη του $10 = 2 \cdot 5$ που το διαιρεί. Εφόσον $\left\lfloor \frac{83}{2^i} \right\rfloor \geq \left\lfloor \frac{83}{5^i} \right\rfloor$, για κάθε $i = 1, 2, \ldots$, αρκεί να βρούμε τη μέγιστη δύναμη του 5 που διαιρεί το $83!$ Έχουμε, $\left\lfloor \frac{83}{5} \right\rfloor + \left\lfloor \frac{83}{25} \right\rfloor = 16+3 = 19$, άρα 5^{19} είναι η μεγαλύτερη δύναμη του 5 που διαιρεί το $83!$ Συνεπώς 10^{19} είναι η μεγαλύτερη δύναμη του 10 που διαιρεί το $83!$, δηλαδή το $83!$ έχει στο τέλος ακριβώς 19 μηδενικά.
(ii) Όπως προηγουμένως, εφόσον $\left\lfloor \frac{n}{2^i} \right\rfloor \geq \left\lfloor \frac{n}{5^i} \right\rfloor$, για κάθε $i = 1, 2, \ldots$, θα πρέπει $\sum_{i=1}^{\infty} \left\lfloor \frac{n}{5^i} \right\rfloor = 26$. Αν π είναι το πηλίκο της διαίρεσης του n δια του 5, τότε $\pi = \left\lfloor \frac{n}{5} \right\rfloor$. (Βλέπε σχόλια μετά την απόδειξη της ταυτότητας της ευκλείδειας διαίρεσης-θεώρημα 1.3). Επειδή $\left\lfloor \frac{\pi}{5} \right\rfloor = \left\lfloor \frac{\lfloor n/5 \rfloor}{5} \right\rfloor = \left\lfloor \frac{n/5}{5} \right\rfloor = \left\lfloor \frac{n}{25} \right\rfloor$ (άσκηση Γ'.3), ο αριθμός $\left\lfloor \frac{n}{25} \right\rfloor$ είναι το πηλίκο π_1 της διαίρεσης του π δια του 5. Ομοίως, ο $\left\lfloor \frac{n}{125} \right\rfloor$ είναι το πηλίκο π_2 της διαίρεσης του π_1 δια του 5. Έστω $n = 5\pi + \upsilon$, $\pi = 5\pi_1 + \upsilon_1$ και $\pi_1 = 5\pi_2 + \upsilon_2$ οι ταυτότητες των ευκλειδείων διαιρέσεων $n : 5$, $\pi : 5$ και $\pi_1 : 5$, αντίστοιχα. Υποθέτουμε ότι $\pi_2 > 0$. Τότε $\pi \geq 5\pi_1 \geq 25\pi_2$. Άρα $\pi + \pi_1 + \pi_2 \geq 25\pi_2 + 5\pi_2 + \pi_2 = 31\pi_2 > 31$, άτοπο γιατί η μεγαλύτερη δύναμη του 5 που διαιρεί το $n!$ θα πρέπει να είναι $26 < 31$. Επομένως $\pi_2 = \left\lfloor \frac{n}{125} \right\rfloor = 0$ και κατά συνέπεια $26 = \pi + \pi_1 \geq 5\pi_1 + \pi_1 = 6\pi_1 \Rightarrow \pi_1 \leq 4$. Συμπεραίνουμε λοιπόν ότι $\pi = 26 - \pi_1 \geq 22$ και άρα $\pi_1 \geq \left\lfloor \frac{22}{5} \right\rfloor = 4$. Τελικώς $\pi = 22$ και $\pi_1 = 4$. Άρα $n = 5 \cdot 22 + \upsilon = 110 + \upsilon$, όπου $0 \leq \upsilon < 5$. Οι δυνατές τιμές για το n είναι λοιπόν: 110, 111, 112, 113 και 114.
(iii) Σύμφωνα με την ανάλυση που έγινε στο προηγούμενο ερώτημα, θα πρέπει το πηλίκο $\pi_3 = \left\lfloor \frac{n}{625} \right\rfloor$ της διαίρεσης του $\pi_2 = \left\lfloor \frac{n}{125} \right\rfloor$ δια του 5 να είναι μηδέν. Αν $\pi_2 = 0$, τότε $36 = \pi + \pi_1 \geq 5\pi_1 + \pi_1 = 6\pi_1 \Rightarrow$ $\Rightarrow \pi_1 \leq 5 \Rightarrow \pi \geq 35 - 5 = 30$ και άρα $\pi_1 \geq \left\lfloor \frac{30}{5} \right\rfloor = 6$, άτοπο. Άρα δεν υπάρχουν n τέτοια, ώστε το $n!$ να τελειώνει σε 36 μηδενικά. ■

Άσκηση 46. Δείξτε ότι η επόμενη εικασία δεν είναι αληθής: Κάθε θετικός ακέραιος μπορεί να γραφεί στη μορφή $p + \alpha^2$, όπου p πρώτος ή 1 και $\alpha \geq 0$.
Απόδειξη: Κατ' αρχάς αποκλείονται οι πρώτοι ως αντιπαραδείγματα, γιατί ένας πρώτος p γράφεται προφανώς στη μορφή $p + 0^2$. Έχουμε $1 = 1 + 0^2$, $4 = 3 + 1^2$, $6 = 5 + 1^2$, $8 = 7 + 1^2$, $9 = 5 + 2^2$, $10 = 1 + 3^2$, $12 = 11 + 1^2$, $14 = 13 + 1^2$, $15 = 11 + 2^2$, $16 = 7 + 3^2$, $18 = 17 + 1^2$, $20 = 19 + 1^2$, $21 = 17 + 2^2$, $22 = 13 + 3^2$, $24 = 23 + 1^2$. Από το 25 αφαιρούμε τετράγωνα και εξετάζουμε αν η διαφορά είναι πρώτος ή 1. Έχουμε $25 - 0^2 = 25$, $25 - 1^2 = 24$, $25 - 2^2 = 21$, $25 - 3^2 = 16$, $25 - 4^2 = 9$ και $25 - 5^2 = 0$. Ο 25 αποτελεί αντιπαράδειγμα για την εικασία αυτή. ■

Άσκηση 47. Αν $n > 1$ δεν είναι της μορφής $6k+3$, τότε ο αριθμός n^2+2^n είναι σύνθετος.
Απόδειξη: Οι δυνατές περιπτώσεις είναι: $n = 6k+1$, $n = 6k+2$, $n = 6k+4$ και $n = 6k+5$. Εξετάζουμε κάθε μία ξεχωριστά. Αν $n = 6k+1$, τότε $n^2 = 36k^2+12k+1 = 6k\cdot(6k+2)+1$. Άρα $n^2+2^n = 6k\cdot(6k+2)+2^{6k+1}+1 = 6k\cdot(6k+2)+2^n+1$. Ο αριθμός $n = 6k+1$ είναι περιττός και συνεπώς $2^n+1 = (2+1)(2^{n-1}-2^{n-2}+\cdots+1)$, δηλαδή $3 \mid 2^n+1$. Άρα $3 \mid n^2+2^n > 3$, γιατί $n > 1$. Ομοίως, αν $n = 6k+5$, τότε ο n είναι περιττός και συνεπώς $3 \mid 2^n+1$. Επίσης, $n^2 = 36k^2+60k+25 = 6(6k^2+10k+4)+1$, δηλαδή $3 \mid n^2-1$. Άρα $3 \mid n^2-1+2^n+1 = n^2+2^n$. Στις περιπτώσεις $n = 6k+2$, $n = 6k+4$ έχουμε $2 \mid n \Rightarrow 2 \mid n^2$ και προφανώς $2 \mid 2^n$. Άρα $2 \mid n^2+2^n$. Σε κάθε περίπτωση ο αριθμός $n^2+2^n \geq 2^2+2^2 = 8$ διαιρείται από το 2 ή το 3 και κατά συνέπεια δεν είναι πρώτος. ■

Άσκηση 48. Να αποδείξετε ότι αν $n > 1$, τότε ο αριθμός $1+\dfrac{1}{2}+\dfrac{1}{3}+\cdots+\dfrac{1}{n}$ δεν είναι ακέραιος.
Απόδειξη: Έστω ϵ το ελάχιστο κοινό πολλαπλάσιο των παρονομαστών $1, 2, 3, \ldots, n$. Έστω επίσης 2^κ η μεγαλύτερη δύναμη του 2 που δεν υπερβαίνει τον n, δηλαδή $2^\kappa \leq n < 2^{\kappa+1}$. Επειδή $n \geq 2 = 2^1$, το κ είναι μεγαλύτερο ή ίσο του 1. Επίσης ο $2^\kappa \leq n$ είναι κάποιος από τους $1, 2, \ldots, n$. Από τους αριθμούς 1, 2, 3, …, n μόνον ο 2^κ διαιρείται από τον 2^κ. Πράγματι, αν $2^\kappa \mid m \leq n$, τότε ο m θα ήταν της μορφής $m = 2^\kappa\mu \leq n$. Αν τώρα $\mu \geq 2$, τότε θα είχαμε $n \geq m = 2^\kappa\mu \geq 2^\kappa\cdot 2 = 2^{\kappa+1}$, άτοπο. Επομένως $\mu = 1$. Συμπεραίνουμε λοιπόν ότι ο αριθμός m είναι αναγκαστικά ο 2^κ.
Προκύπτουν λοιπόν δύο πράγματα. **1ο:** Το 2^κ, ως η μεγαλύτερη δύναμη που διαιρεί κάποιον από τους $1, 2, \ldots, n$, είναι και η μεγαλύτερη δύναμη που διαιρεί το ελάχιστο κοινό πολλαπλάσιό τους ϵ. Επομένως το ϵ γράφεται στη μορφή $2^\kappa\cdot\lambda$, όπου λ περιττός. **2ο:** Από τους αριθμούς $1, 2, \ldots, n$, μόνον ο ίδιος ο 2^κ διαιρείται από τον 2^κ. Κάθε άλλος $m \leq n$ θα γράφεται στη μορφή $2^{\beta_m}\cdot\rho_m$, όπου $0 \leq \beta_m < \kappa$ και ρ_m περιττός. Επειδή όμως $m = 2^{\beta_m}\cdot\rho_m \mid \epsilon = 2^\kappa\cdot\lambda$ και ρ_m, λ περιττοί, θα έχουμε $\rho_m \mid \lambda$ και άρα $\tau_m := \dfrac{\lambda}{\rho_m} \in \mathbb{Z}$.
Επομένως $\dfrac{1}{m} = \dfrac{\epsilon/m}{\epsilon} = \dfrac{2^{\kappa-\beta_m}\cdot\tau_m}{2^\kappa\cdot\lambda}$ με $\kappa > \beta_m$ και άρα ο αριθμός $2^{\kappa-\beta_m}\cdot\tau_m$ είναι άρτιος.
Συμπέρασμα: $1+\dfrac{1}{2}+\dfrac{1}{3}+\cdots+\dfrac{1}{\boxed{2^\kappa}}+\cdots+\dfrac{1}{n} = \dfrac{2^{\kappa-\beta_1}\cdot\tau_1+2^{\kappa-\beta_2}\cdot\tau_2+2^{\kappa-\beta_3}\cdot\tau_3+\cdots+\boxed{\lambda}+\cdots+2^{\kappa-\beta_n}\cdot\tau_n}{2^\kappa\cdot\lambda}$
είναι ένα κλάσμα με περιττό αριθμητή και άρτιο παρονομαστή. Επομένως το κλάσμα αυτό δεν είναι ακέραιος. ■

Άσκηση 49. Έστω m και n θετικοί ακέραιοι. Δείξτε ότι:
(i) $m!\cdot(n!)^m \mid (mn)!$
(ii) $m!n!(m+n)! \mid (2m)!\cdot(2n)!$
Απόδειξη: (i) 1η απόδειξη: Έστω p πρώτος. Η μεγαλύτερη δύναμη του p που διαιρεί το $m!$ είναι p^α, όπου $\alpha = \sum\limits_{i=1}^{\infty}\left\lfloor\dfrac{m}{p^i}\right\rfloor$ και η μεγαλύτερη δύναμη του p που διαιρεί το $n!$ είναι p^β, όπου $\beta = \sum\limits_{i=1}^{\infty}\left\lfloor\dfrac{n}{p^i}\right\rfloor$. Επομένως η μεγαλύτερη δύναμη του p που διαιρεί το $m!\cdot(n!)^m$ είναι $p^{\alpha+m\beta}$. Ομοίως, η μεγαλύτερη δύναμη του p που διαιρεί το $(mn)!$ είναι p^γ, όπου $\gamma = \sum\limits_{i=1}^{\infty}\left\lfloor\dfrac{mn}{p^i}\right\rfloor$. Αρκεί να δείξουμε ότι $\alpha+m\beta \leq \gamma \Leftrightarrow \sum\limits_{i=1}^{\infty}\left(\left\lfloor\dfrac{m}{p^i}\right\rfloor+m\left\lfloor\dfrac{n}{p^i}\right\rfloor\right) \leq \sum\limits_{i=1}^{\infty}\left\lfloor\dfrac{mn}{p^i}\right\rfloor$. Αν $p > n$, τότε $\left\lfloor\dfrac{n}{p^i}\right\rfloor = 0$, οπότε η αποδεικτέα σχέση γίνεται $\sum\limits_{i=1}^{\infty}\left\lfloor\dfrac{m}{p^i}\right\rfloor \leq \sum\limits_{i=1}^{\infty}\left\lfloor\dfrac{mn}{p^i}\right\rfloor$, η οποία προφανώς ισχύει γιατί $\dfrac{m}{p^i} \leq \dfrac{mn}{p^i}$, για κάθε $i = 1, 2, \ldots$ Έστω τώρα p^λ η μεγαλύτερη δύναμη του p που δεν υπερβαίνει τον n. Παρατηρούμε ότι $\left\lfloor\dfrac{n}{p^i}\right\rfloor \leq \dfrac{n}{p^i} \Rightarrow m\left\lfloor\dfrac{n}{p^i}\right\rfloor \leq \dfrac{mn}{p^i} \Rightarrow m\left\lfloor\dfrac{n}{p^i}\right\rfloor \leq \left\lfloor\dfrac{mn}{p^i}\right\rfloor$, για κάθε $i = 1, 2, \ldots, \lambda$. Συνεπώς $m\sum\limits_{i=1}^{\infty}\left\lfloor\dfrac{n}{p^i}\right\rfloor = m\sum\limits_{i=1}^{\lambda}\left\lfloor\dfrac{n}{p^i}\right\rfloor \leq \sum\limits_{i=1}^{\lambda}\left\lfloor\dfrac{mn}{p^i}\right\rfloor$. Ακόμη $\dfrac{m}{p^i} \leq \dfrac{m}{p^i}\dfrac{n}{p^\lambda} = \dfrac{mn}{p^{\lambda+i}}$ και επομένως $\left\lfloor\dfrac{m}{p^i}\right\rfloor \leq \left\lfloor\dfrac{mn}{p^{\lambda+i}}\right\rfloor$, για κάθε $i = 1, 2, \ldots$ Άρα $\sum\limits_{i=1}^{\infty}\left\lfloor\dfrac{m}{p^i}\right\rfloor \leq \sum\limits_{i=\lambda+1}^{\infty}\left\lfloor\dfrac{mn}{p^i}\right\rfloor$ Τελικώς $\sum\limits_{i=1}^{\infty}\left\lfloor\dfrac{m}{p^i}\right\rfloor + m\sum\limits_{i=1}^{\infty}\left\lfloor\dfrac{n}{p^i}\right\rfloor \leq$

$$\leq \sum_{i=\lambda+1}^{\infty} \left\lfloor \frac{mn}{p^i} \right\rfloor + \sum_{i=1}^{\lambda} \left\lfloor \frac{mn}{p^i} \right\rfloor = \sum_{i=1}^{\infty} \left\lfloor \frac{mn}{p^i} \right\rfloor.$$

2η απόδειξη: Για κάθε $k = 1, 2, \ldots, m$ το $(n-1)!$ διαιρεί το γινόμενο των $n-1$ διαδοχικών αριθμών $((k-1)n+1)((k-1)n+2)\cdots((k-1)n+n-1)$. Σημειώνουμε ότι $(k-1)n+n-1 = kn-1$. Επομένως $k \cdot n! \mid ((k-1)n+1)((k-1)n+2)\cdots((k-1)n+n-1)(kn)$, για κάθε $k = 1, 2, \ldots, m$.
Πολλαπλασιάζοντας κατά μέλη παίρνουμε: $1 \cdot n! \cdot 2 \cdot n! \cdot 3 \cdot n! \cdots m \cdot n! \mid 1 \cdot 2 \cdots n \cdot (n+1)(n+2)\cdots(2n)\cdots((m-1)n+1)((m-1)n+2)\cdots(mn) \Leftrightarrow m! \cdot (n!)^m \mid (mn)!$

(ii) Για κάθε πρώτο p έχουμε: $\dfrac{m}{p^i} + \dfrac{n}{p^i} + \dfrac{m+n}{p^i} = \dfrac{2m}{p^i} + \dfrac{2n}{p^i}$.
Γνωρίζουμε ότι (άσκηση Γ.2-παράρτημα Γ) ότι $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$, για κάθε $x, y \in \mathbb{R}$. Αν λοιπόν $2\left\lfloor \frac{m}{p^i} \right\rfloor = \left\lfloor \frac{2m}{p^i} \right\rfloor$ και $2\left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{2n}{p^i} \right\rfloor$, τότε θα έχουμε $2\left\lfloor \frac{m}{p^i} \right\rfloor \leq \frac{2m}{p^i} < 2\left\lfloor \frac{m}{p^i} \right\rfloor + 1$ και $2\left\lfloor \frac{n}{p^i} \right\rfloor \leq \frac{2n}{p^i} < 2\left\lfloor \frac{n}{p^i} \right\rfloor + 1$, οπότε $2\left\lfloor \frac{m}{p^i} \right\rfloor + 2\left\lfloor \frac{n}{p^i} \right\rfloor \leq \frac{2(m+n)}{p^i} < 2\left\lfloor \frac{m}{p^i} \right\rfloor + 2\left\lfloor \frac{n}{p^i} \right\rfloor + 2 \Leftrightarrow \left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor \leq \frac{m+n}{p^i} < \left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor + 1$, δηλαδή $\left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{m+n}{p^i} \right\rfloor$. Σ' αυτή την περίπτωση θα έχουμε: $\left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor + \left\lfloor \frac{m+n}{p^i} \right\rfloor = \left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor + \left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor = 2\left\lfloor \frac{m}{p^i} \right\rfloor + 2\left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{2m}{p^i} \right\rfloor + \left\lfloor \frac{2n}{p^i} \right\rfloor$. Αν τώρα $\left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{m+n}{p^i} \right\rfloor - 1$, τότε δεν μπορεί να έχουμε ταυτόχρονα $2\left\lfloor \frac{m}{p^i} \right\rfloor = \left\lfloor \frac{2m}{p^i} \right\rfloor$ και $2\left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{2n}{p^i} \right\rfloor$. Άρα $2\left\lfloor \frac{m}{p^i} \right\rfloor = \left\lfloor \frac{2m}{p^i} \right\rfloor - 1$ ή $2\left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{2n}{p^i} \right\rfloor - 1$. Σε κάθε περίπτωση $2\left\lfloor \frac{m}{p^i} \right\rfloor + 2\left\lfloor \frac{n}{p^i} \right\rfloor \leq \left\lfloor \frac{2m}{p^i} \right\rfloor + \left\lfloor \frac{2n}{p^i} \right\rfloor - 1$. Τότε όμως θα έχουμε: $\left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor + \left\lfloor \frac{m+n}{p^i} \right\rfloor = \left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor + \left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor + 1 = 2\left\lfloor \frac{m}{p^i} \right\rfloor + 2\left\lfloor \frac{n}{p^i} \right\rfloor + 1 \leq \left\lfloor \frac{2m}{p^i} \right\rfloor + \left\lfloor \frac{2n}{p^i} \right\rfloor - 1 + 1 = \left\lfloor \frac{2m}{p^i} \right\rfloor + \left\lfloor \frac{2n}{p^i} \right\rfloor$. ■

ΑΛΥΤΕΣ ΑΣΚΗΣΕΙΣ

38. Λύστε την άσκηση 35 (σελ. 28) χρησιμοποιώντας πρώτους αριθμούς.

39. Αναλύστε σε γινόμενο πρώτων παραγόντων τους αριθμούς 79860, 4851 και 20475. Στη συνέχεια βρείτε τον $(79860, 4851, 20475)$ και το $[79860, 4851, 20475]$.

40. Δείξτε τα παρακάτω:
(i) Κάθε πρώτος της μορφής $3n+1$ είναι επίσης της μορφής $6k+1$.
(ii) Κάθε ακέραιος της μορφής $3n+2$, όπου $n > 0$, έχει έναν πρώτο διαιρέτη της ίδιας μορφής.
(iii) Ο μοναδικός πρώτος της μορφής $n^3 - 1$ είναι ο 7.
(iv) Ο μοναδικός πρώτος p για τον οποίο ο $3p+1$ είναι τέλειο τετράγωνο είναι ο 5.
(v) Ο μοναδικός πρώτος της μορφής $n^2 - 4$ είναι ο 5.

41. Αν $p \geq 5$ είναι πρώτος αριθμός, τότε ο $p^2 + 2$ είναι σύνθετος.

42. Για κάθε ακέραιο $n > 1$, ο αριθμός $n^4 + 4$ είναι σύνθετος.

43. Αν ο $p > 2$ είναι πρώτος και $1 < k < p$, τότε $p \mid \binom{p}{k}$.

44. Να βρεθούν όλοι οι πρώτοι παράγοντες του $50!$ Στη συνέχεια αναλύστε τον $50!$ σε γινόμενο πρώτων παραγόντων.

45. Ποιοι από τους παρακάτω αριθμούς είναι πρώτοι και ποιοι σύνθετοι;
353, 379, 403, 439, 451, 499, 769, 899.

46. Βρείτε τη μεγαλύτερη δύναμη του 21 που διαιρεί το $\binom{1325}{660}$.

47. **(i)** Να βρεθεί ο πρώτος p, ώστε ο ακέραιος $31p+1$ να είναι τέλειο τετράγωνο.
(ii) Να βρεθεί ο πρώτος p, ώστε ο ακέραιος $23p+4$ να είναι τέλειο τετράγωνο.
(iii) Να βρεθεί ο πρώτος p, ώστε ο ακέραιος $8p+9$ να είναι τέλειο τετράγωνο.
(iv) Να βρεθεί ο πρώτος p, ώστε ο ακέραιος $5p+16$ να είναι τέλειο τετράγωνο.

48. **(i)** Αν $p \geq q \geq 5$ είναι πρώτοι, δείξτε ότι $24 \mid p^2 - q^2$.
(ii) Αν $p \neq 5$ είναι περιττός πρώτος, δείξτε ότι κάποιος από τους p^2-1 ή p^2+1 διαιρείται με το 10.

49. Δώστε μια άλλη απόδειξη της απειρίας των πρώτων αριθμών, ως εξής: Υποθέτουμε ότι όλοι οι πρώτοι είναι οι $p_1, p_2, \ldots, p_n$. Θεωρήστε έναν πρώτο διαιρέτη του αριθμού $\mathrm{N} = p_2p_3\cdots p_n + p_1p_3\cdots p_n + \cdots + +p_1p_2\cdots p_{n-1}$.

50. Βρείτε όλα τα ζεύγη των πρώτων αριθμών (p,q) με $p-q=3$.

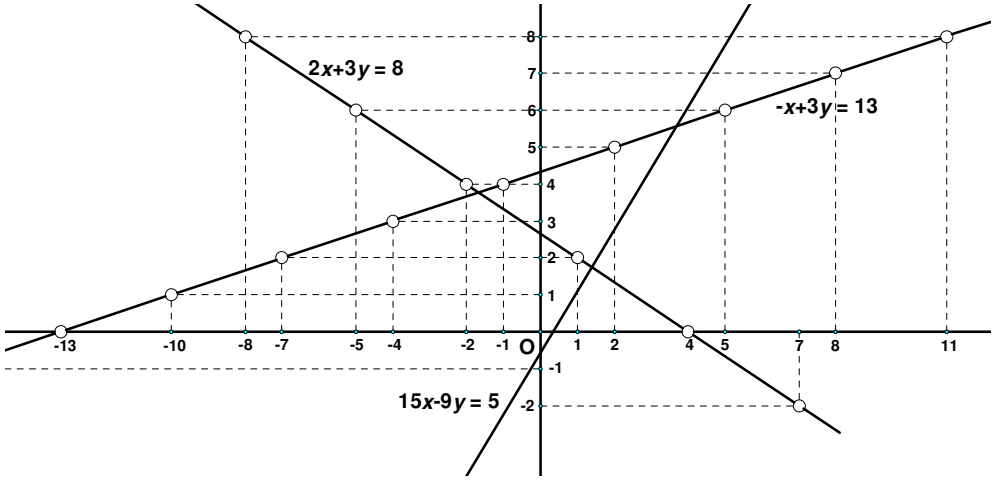
51. Έστω $p_1 < p_2 < p_3 \cdots$ η ακολουθία των πρώτων αριθμών. Τότε
(i) $p_n > 2n-1$, για κάθε $n \geq 5$.
(ii) Κανείς από τους ακεραίους της μορφής $P_n = p_1p_2\cdots p_n + 1$ δεν είναι τέλειο τετράγωνο.
(iii) Το άθροισμα $\dfrac{1}{p_1} + \dfrac{1}{p_2} + \cdots + \dfrac{1}{p_n}$ δεν είναι ποτέ ακέραιος.

52. Δύο θετικοί ακέραιοι έχουν άθροισμα 27 και ελάχιστο κοινό πολλαπλάσιο 60. Βρείτε τους αριθμούς αυτούς.

53. Έστω p και q πρώτοι τέτοιοι, ώστε $p+q=(p-q)^3$. Βρείτε τους πρώτους αυτούς.

1.4 Η γραμμική διοφαντική[1] εξίσωση $ax+\beta y=\gamma$

Έστω $\alpha, \beta, \gamma \in \mathbb{Z}$ με $\alpha^2+\beta^2 > 0$. Από τα σχολικά μας χρόνια ξέρουμε ότι η εξίσωση $\alpha x + \beta y = \gamma$ ορίζει στο επίπεδο μια ευθεία. Τίθεται το ερώτημα: Πότε μια τέτοια ευθεία διέρχεται από σημεία του επιπέδου, τα οποία έχουν ακέραιες συντεταγμένες; Τα σημεία αυτά λέγονται διεθνώς lattice-points. Ισοδύναμα, το ερώτημα τίθεται ως εξής: Υπάρχουν ζεύγη (x,y) ακεραίων αριθμών που επαληθεύουν την εξίσωση $\alpha x + \beta y = \gamma$; Αν ναι, υπάρχει τύπος που να μας δίνει όλες αυτές τις λύσεις;



Σχήμα 3

[1]Προς τιμή του μεγάλου αρχαίου Έλληνα μαθηματικού Διοφάντου του Αλεξανδρέως (περίπου 210 – 290 μ.Χ.). Το έργο του «Αριθμητικά» απετέλεσε πηγή έμπνευσης για τον μεγάλο Γάλλο μαθηματικό Pierre de Fermat (1607–1665). Μελετώντας στο έργο αυτό τη λύση για τις πυθαγόρειες τριάδες, ο Fermat ισχυρίστηκε ότι απέδειξε ότι η εξίσωση $x^n + y^n = z^n$, όπου $n > 2$ δεν έχει ακέραιες λύσεις. Το πρόβλημα αυτό έμεινε στην ιστορία ως «το μεγάλο θεώρημα του Fermat». Σχεδόν μετά από 350 χρόνια, και συγκεκριμένα το 1995, ο Andrew Wiles απέδειξε τον ισχυρισμό αυτό. Ο Wiles (τελικώς και με τη βοήθεια του Richard Taylor) χρησιμοποίησε προχωρημένες μαθηματικές θεωρίες, αποδεικνύοντας ουσιαστικά μια μερική περίπτωση της περίφημης εικασίας Taniyama–Shimura.

Παρατηρούμε στο προηγούμενο σχήμα ότι οι ευθείες $2x+3y=8$ και $-x+3y=13$ έχουν ακέραιες λύσεις. Η ευθεία $15x-9y=5$ δεν έχει ακέραιες λύσεις.

Θεώρημα 1.54. Θεωρούμε την εξίσωση $\alpha x+\beta y=\gamma$, όπου $\alpha,\beta,\gamma\in\mathbb{Z}$ και $\alpha^2+\beta^2>0$. Έστω $\delta=(\alpha,\beta)$.
(i) Αναγκαία και ικανή συνθήκη ώστε η εξίσωση $\alpha x+\beta y=\gamma$ να έχει ακέραιες λύσεις είναι **το δ να διαιρεί το γ**.
(ii) Αν (x_0,y_0) είναι μια ακέραια λύση της $\alpha x+\beta y=\gamma$, τότε κάθε άλλη ακέραια λύση (x,y) αυτής δίνεται από τον τύπο: $\begin{cases} x=x_0-\dfrac{\beta}{\delta}\cdot t \\ y=y_0+\dfrac{\alpha}{\delta}\cdot t \end{cases}$, $t\in\mathbb{Z}$

Απόδειξη: (i) Αναγκαία: Αν υπάρχει ακέραια λύση (x,y) της εξίσωσης $\alpha x+\beta y=\gamma$, τότε επειδή $\delta\mid\alpha$ και $\delta\mid\beta$, θα έχουμε $\delta\mid\alpha x+\beta y=\gamma$.
Ικανή: Έστω $\delta\mid\gamma$. Γνωρίζουμε ότι ο μέγιστος κοινός διαιρέτης δ των α και β γράφεται ως γραμμικός συνδυασμός των α και β. Έστω λοιπόν $\alpha x'+\beta y'=\delta$, όπου $x',y'\in\mathbb{Z}$. Εφόσον $\lambda:=\dfrac{\gamma}{\delta}\in\mathbb{Z}$, πολλαπλασιάζουμε τη σχέση $\alpha x'+\beta y'=\delta$ με λ και παίρνουμε $\alpha\lambda x'+\beta\lambda y'=\lambda\delta\Leftrightarrow\Leftrightarrow\alpha x+\beta y=\gamma$, όπου $x=\lambda x'$ και $y=\lambda y'$.
(ii) Έστω (x_0,y_0) μια ακέραια λύση της $\alpha x+\beta y=\gamma$. Αν (x,y) είναι μια οποιαδήποτε ακέραια λύση της εξίσωσης αυτής, τότε θα έχουμε: $\alpha x+\beta y=\alpha x_0+\beta y_0\Leftrightarrow\beta(y-y_0)=\alpha(x_0-x)\Leftrightarrow\dfrac{\beta}{\delta}(y-y_0)=\dfrac{\alpha}{\delta}(x_0-x)$. Επομένως $\dfrac{\beta}{\delta}\;\Big|\;\dfrac{\alpha}{\delta}(x_0-x)\underset{\left(\frac{\beta}{\delta},\frac{\alpha}{\delta}\right)=1}{\Leftrightarrow}\dfrac{\beta}{\delta}\;\Big|\;x_0-x$. Άρα το x_0-x είναι της μορφής $t\cdot\dfrac{\beta}{\delta}$, με $t\in\mathbb{Z}$. Επομένως $x=x_0-t\cdot\dfrac{\beta}{\delta}$. Αν αντικαταστήσουμε την τιμή $x_0-x=t\cdot\dfrac{\beta}{\delta}$ στην εξίσωση $\dfrac{\beta}{\delta}(y-y_0)=\dfrac{\alpha}{\delta}(x_0-x)$, θα πάρουμε $\dfrac{\beta}{\delta}(y-y_0)=\dfrac{\alpha}{\delta}\cdot t\cdot\dfrac{\beta}{\delta}\Leftrightarrow y=y_0+t\cdot\dfrac{\alpha}{\delta}$. Πράγματι, για κάθε $t\in\mathbb{Z}$ έχουμε:

$$\alpha\Big(x_0-t\cdot\frac{\beta}{\delta}\Big)+\beta\Big(y_0+t\cdot\frac{\alpha}{\delta}\Big)=\alpha x_0-\frac{t\alpha\beta}{\delta}+\beta y_0+\frac{t\alpha\beta}{\delta}=\alpha x_0+\beta y_0=\gamma.$$ ■

Άσκηση 50. Να λυθεί στο $\mathbb{Z}$ η γραμμική εξίσωση $360x+1617y=12$.
Λύση: Παρατηρούμε ότι $360=2^3\cdot3^2\cdot5$ και $1617=3\cdot7^2\cdot11$. Επομένως $(360,21)=3\mid12$ και κατά συνέπεια η εξίσωση έχει ακέραιες λύσεις. Χρησιμοποιούμε τον αλγόριθμο του Ευκλείδη για να εκφράσουμε το 3 ως γραμμικό συνδυασμό των 360 και 1617. Έχουμε: $1617=4\cdot360+177$, $360=2\cdot177+6$ και $177=29\cdot6+3$. Άρα $3=177-29\cdot6=177-29(360-2\cdot177)=-29\cdot360+59\cdot177=-29\cdot360+59(1617-4\cdot360)=$ $=59\cdot1617-(29+4\cdot59)\cdot360=(-265)\cdot360+59\cdot1617$. Επομένως $12=360\cdot(-265)\cdot4+1617\cdot(59\cdot4)=$ $=360\cdot(-1060)+1617\cdot236$. Έχουμε βρει λοιπόν τη λύση $(x_0,y_0)=(-1060,236)$. Ακόμη, $\dfrac{1617}{3}=539$ και $\dfrac{360}{3}=120$. Η γενική λύση της εξίσωσης είναι: $(x,y)=(-1060-539t,236+120t)$, όπου $t\in\mathbb{Z}$. ■

Άσκηση 51. Να βρεθούν οι θετικές ακέραιες λύσεις (αν υπάρχουν) της εξίσωσης: $12x+30y=66$.
Λύση: Παρατηρούμε ότι $(12,30)=(2^2\cdot3,2\cdot3\cdot5)=6\mid66$. Άρα η εξίσωση έχει ακέραιες λύσεις. Εφαρμόζουμε τον αλγόριθμο του Ευκλείδη: $30=2\cdot12+6$, $12=2\cdot6$. Επομένως $6=30-2\cdot12=$ $=(-2)12+1\cdot30$. Άρα $(-22)12+11\cdot30=66$. Μια λύση είναι λοιπόν η $(x_0,y_0)=(-22,11)$. Η γενική λύση είναι λοιπόν $(x,y)=\Big(-22-t\cdot\dfrac{30}{6},11+t\cdot\dfrac{12}{6}\Big)=(-22-5t,11+2t)$, όπου $t\in\mathbb{Z}$.
Θα πρέπει λοιπόν $-22-5t>0\Leftrightarrow t<-\dfrac{22}{5}\Leftrightarrow t\le-5$. Επίσης $11+2t>0\Leftrightarrow t>-\dfrac{11}{2}\Leftrightarrow t\ge-5$. Η μοναδική θετική λύση προκύπτει για $t=-5$ και είναι η: $x=-22-5(-5)=3$, $y=11+2(-5)=1$. ■

Άσκηση 52. Έστω α,β,γ μη μηδενικοί ακέραιοι και $\delta\in\mathbb{Z}$.
(i) Δείξτε ικανή και αναγκαία συνθήκη ότι για να έχει η εξίσωση $\alpha x+\beta y+\gamma z=\delta$ ακέραιες λύσεις είναι η $(\alpha,\beta,\gamma)\mid\delta$.
(ii) Αν η εξίσωση $\alpha x+\beta y+\gamma z=\delta$ έχει ακέραιες λύσεις, βρείτε τη γενική μορφή των λύσεων αυτών.
Λύση: (i) Έστω $\delta_1=(\alpha,\beta,\gamma)$. Αν η εξίσωση $\alpha x+\beta y+\gamma z=\delta$ έχει ακέραιες λύσεις και (x,y,x) είναι μία

από αυτές, τότε $\delta_1 \mid \alpha$, $\delta_1 \mid \beta$ και $\delta_1 \mid \gamma$, οπότε $\delta_1 \mid \alpha x+\beta y+\gamma z = \delta$. Αντιστρόφως, υποθέτουμε ότι $\delta_1 \mid \delta$ και $\delta = \lambda\delta_1,\ \lambda \in \mathbb{Z}$. Εφόσον $\delta_1 = (\alpha, \beta, \gamma)$, υπάρχουν ακέραιοι x_1, y_1, z_1 τέτοιοι, ώστε $\alpha x_1 + \beta y_1 + \gamma z_1 = \delta_1$ και κατά συνέπεια $\alpha(\lambda x_1) + \beta(\lambda y_1) + \gamma(\lambda z_1) = \lambda\delta_1 = \delta$.

(ii) Έστω (x, y, z) μια ακέραια λύση της $\alpha x+\beta y+\gamma z = \delta$. Ο ακέραιος $\alpha x+\beta y$ είναι γραμμικός συνδυασμός των α και β, άρα πολλαπλάσιο του (α, β). Έστω $\alpha x + \beta y = \omega \cdot (\alpha, \beta)$. Η εξίσωση $\alpha x + \beta y + \gamma z = \delta$ λοιπόν γίνεται: $(\alpha, \beta)\omega + \gamma z = \delta$. Αν (ω_0, z_0) είναι μια λύση της $(\alpha, \beta)\omega + \gamma z = \delta$, τότε η γενική λύση της $(\alpha, \beta)\omega + \gamma z = \delta$ είναι της μορφής $(\omega, z) = \left(\omega_0 - t \cdot \dfrac{\gamma}{(\alpha, \beta, \gamma)}, z_0 + t \cdot \dfrac{(\alpha, \beta)}{(\alpha, \beta, \gamma)}\right),\ t \in \mathbb{Z}$.

Τώρα, αν $\alpha x_1 + \beta y_1 = (\alpha, \beta)$ θα έχουμε $\alpha(x_1\omega) + \beta(y_1\omega) = (\alpha, \beta)\omega$. Κάθε άλλη λύση της $\alpha x + \beta y = (\alpha, \beta)\omega$ είναι της μορφής $\begin{cases} x = x_1\omega - s \cdot \dfrac{\beta}{(\alpha, \beta)} \\ y = y_1\omega + s \cdot \dfrac{\alpha}{(\alpha, \beta)} \end{cases}$, $s \in \mathbb{Z}$ και αν αντικαταστήσουμε το ω με $\omega_0 - t \cdot \dfrac{\gamma}{(\alpha, \beta, \gamma)}$, θα πάρουμε

$$\begin{cases} x = x_1\omega_0 - t \cdot \dfrac{x_1\gamma}{(\alpha, \beta, \gamma)} - s \cdot \dfrac{\beta}{(\alpha, \beta)} \\ y = y_1\omega_0 - t \cdot \dfrac{y_1\gamma}{(\alpha, \beta, \gamma)} + s \cdot \dfrac{\alpha}{(\alpha, \beta)} \\ z = z_0 + t \cdot \dfrac{(\alpha, \beta)}{(\alpha, \beta, \gamma)} \end{cases},\ t, s \in \mathbb{Z} \qquad \textbf{(1)}$$ ■

Άσκηση 53. Να λυθεί η γραμμική διοφαντική εξίσωση $18x + 6y + 21z = 33$. Έχει η εξίσωση αυτή θετικές λύσεις;

Λύση: Παρατηρούμε ότι $(18, 6, 21) = (2 \cdot 3^2, 2 \cdot 3, 3 \cdot 7) = 3 \mid 33$. Άρα η εξίσωση έχει λύσεις. Προφανώς $(18, 6) = 6$ και $6 = 18 \cdot 1 + (-2)6$. Θέτουμε $x_1 = 1$ και $y_1 = -2$.

Η αρχική εξίσωση ανάγεται στην $6\omega + 21z = 33$. Με τον αλγόριθμο του Ευκλείδη (μία διαίρεση αρκεί εδώ) γράφουμε το $3 = (6, 21)$ ως γραμμικό συνδυασμό των 6 και 21. Έχουμε $21 = 3 \cdot 6 + 3 \Leftrightarrow (-3) \cdot 6 + 1 \cdot 21 = 3 \Leftrightarrow (-33) \cdot 6 + 11 \cdot 21 = 33$, δηλαδή $\omega_0 = -33$ και $z_0 = 11$. Εφαρμόζουμε τους τύπους **(1)**:

$$\begin{cases} x = 1 \cdot (-33) - t \cdot \dfrac{21}{3} - s \cdot \dfrac{6}{6} = \boxed{-33 - 7t - s} \\ y = (-2)(-33) - t \cdot \dfrac{-2 \cdot 21}{3} + s \cdot \dfrac{18}{6} = \boxed{66 + 14t + 3s} \\ z = 11 + t \cdot \dfrac{6}{3} = \boxed{11 + 2t} \end{cases},\ t, s \in \mathbb{Z}$$

Για να έχει θετικές λύσεις η παραπάνω εξίσωση θα πρέπει $11 + 2t > 0 \Leftrightarrow t > -\dfrac{11}{2} \Leftrightarrow t \geq -5$,

$66 + 14t + 3s > 0 \Leftrightarrow s > -22 - \dfrac{14}{3}t$ και $-33 - 7t - s > 0 \Leftrightarrow s < -33 - 7t$. Επομένως πρέπει $-22 - \dfrac{14}{3}t < -33 - 7t \Leftrightarrow t < -\dfrac{33}{7} \Leftrightarrow t \leq -5$. Επομένως $t = -5$. Άρα $-22 - \dfrac{14}{3} \cdot (-5) < s < -33 - 7 \cdot (-5) \Leftrightarrow$

$\Leftrightarrow 1 < \dfrac{4}{3} < s < 2$, άτοπο γιατί $s \in \mathbb{Z}$. Άρα η εξίσωση δεν έχει θετικές λύσεις. ■

Άσκηση 54. (Euler) Ένας αγρότης υπολόγισε ότι χρειάζεται 1770 κορώνες για να αγοράσει άλογα και βόδια. Κάθε άλογο κοστίζει 31 κορώνες και κάθε βόδι 21 κορώνες. Πόσα άλογα και πόσα βόδια αγόρασε;

Λύση: Προφανώς, αν x είναι το πλήθος των αλόγων και y το πλήθος των βοδιών, έχουμε $31x + 21y = 1770$. Το 31 είναι πρώτος και $21 = 3 \cdot 7$. Επομένως $(31, 21) = 1 \mid 1770$. Η εξίσωση $31x + 21y = 1770$ έχει λοιπόν ακέραιες λύσεις. Έχουμε: $31 = 21+10$, $21 = 2 \cdot 10+1$, άρα $1 = 21-2 \cdot 10 = 21-2 \cdot (31-21) = -2 \cdot 31+3 \cdot 21$. Επομένως $31 \cdot (-2) \cdot 1770 + 21 \cdot 3 \cdot 1770 = 1770 \Leftrightarrow 31 \cdot (-3540) + 21 \cdot 5310 = 1770$.

Η γενική λύση της εξίσωσης $31x + 21y = 1770$ είναι λοιπόν $\begin{cases} x = -3540 - 21t \\ y = 5310 + 31t \end{cases}, t \in \mathbb{Z}$.

Αναζητούμε θετικές λύσεις. Έχουμε $21t < -3540 \Leftrightarrow t < -168 - \dfrac{4}{7} \Leftrightarrow t \leq -169$. Επίσης, $31t > -5310 \Leftrightarrow$

$\Leftrightarrow t > -171 - \dfrac{9}{31} \Leftrightarrow t \geq -171$. Επομένως $t = -171$ ή $t = -170$ ή $t = -169$.

Για $t = -171$ παίρνουμε $x = -3540 + 171 \cdot 21 = 51$ και $y = 5310 - 31 \cdot 171 = 9$, για $t = -170$ παίρνουμε

$x=-3540+170\cdot 21=30$ και $y=5310-31\cdot 170=40$ και για $t=-169$ παίρνουμε $x=-3540+169\cdot 21=9$ και $y=5310-31\cdot 169=71$. ■

Άσκηση 55. (Bhaskara: 1114–1185 μ.Χ.) Δύο άνδρες είναι εξίσου πλούσιοι. Ο ένας έχει 5 ρουμπίνια, 5 μαργαριτάρια και 90 χρυσά νομίσματα. Ο άλλος έχει 8 ρουμπίνια, 9 μαργαριτάρια και 48 χρυσά νομίσματα. Αν τα ρουμπίνια είναι ακριβότερα από τα μαργαριτάρια, βρείτε την αξία σε χρυσά νομίσματα κάθε ρουμπινιού και κάθε μαργαριταριού.

Λύση: Αν η αξία σε χρυσά νομίσματα κάθε ρουμπινιού είναι x και κάθε μαργαριταριού y, τότε έχουμε την εξίσωση $5x+5y+90=8x+9y+48\Leftrightarrow 3x+4y=42$. Προφανώς $\big((3,4)=1\big)$ η εξίσωση $3x+4y=42$ έχει ακέραιες λύσεις. Έχουμε $3\cdot(-1)+4\cdot 1=1\Leftrightarrow 3\cdot(-42)+4\cdot 42=42$. Η γενική λύση της $3x+4y=42$ είναι $\begin{cases} x=-42-4t \\ y=42+3t \end{cases}, t\in\mathbb{Z}$. Πρέπει $-42-4t>0\Leftrightarrow t<-10-\frac{1}{2}\Leftrightarrow t\leq -11$ και $42+3t>0\Leftrightarrow t>-14\Leftrightarrow t\geq -13$. Επομένως $t=-13$ ή $t=-12$ ή $t=-11$. Για $t=-13$, $x=10$ και $y=3$, για $t=-12$, $x=6$ και $y=6$ και για $t=-11$, $x=2$ και $y=9$. Επειδή τα ρουμπίνια είναι ακριβότερα από τα μαργαριτάρια, οι δύο τελευταίες περιπτώσεις αποκλείονται. Επομένως κάθε ρουμπίνι κοστίζει 10 χρυσά νομίσματα και κάθε μαργαριτάρι 3. ■

ΑΛΥΤΕΣ ΑΣΚΗΣΕΙΣ

54. Λύστε τις παρακάτω γραμμικές διοφαντικές εξισώσεις:
(i) $56x+72y=40$.
(ii) $24x+138y=18$.
(iii) $221x+35y=11$.

55. Βρείτε τις θετικές λύσεις (αν φυσικά υπάρχουν) των παρακάτω εξισώσεων:
(i) $18x+5y=48$.
(ii) $54x+21y=906$.
(iii) $123x+360y=99$.
(iv) $158x-57y=7$.

56. Λύστε την εξίσωση $21x+14y+6z=74$. Δείξτε ότι έχει μοναδική θετική λύση.

57. Αν α και β είναι θετικοί ακέραιοι, πρώτοι μεταξύ τους, δείξτε ότι για κάθε $\gamma\in\mathbb{Z}$ η εξίσωση $\alpha x-\beta y=\gamma$ έχει άπειρες θετικές λύσεις.

58. Ένα παιδάκι αγόρασε σοκολάτες και καραμέλες. Κάθε σοκολάτα κοστίζει 2,5€ και κάθε καραμέλα 0,3€. Συνολικά πλήρωσε 13,5€. Πόσες σοκολάτες και πόσες καραμέλες αγόρασε;

59. Τσοπάνος αγόρασε πρόβατα και γίδια. Για κάθε πρόβατο πλήρωσε 65€ και για κάθε γίδι 40€. Συνολικά πλήρωσε 1040€. Πόσα πρόβατα και πόσα γίδια αγόρασε;

60. Για ποιες τιμές του θετικού ακεραίου k ο μέγιστος κοινός διαιρέτης των $9k-7$ και $5k+4$ ισούται με 71;

61. (Christoff Rudolff, 1526) Σε μια παρέα παρευρίσκονται 20 άτομα, άντρες, γυναίκες και παιδιά. Όλοι μαζί πλήρωσαν 20 νομίσματα. Κάθε άνδρας πλήρωσε 3 νομίσματα, κάθε γυναίκα 2 και κάθε παιδί $\frac{1}{2}$. Πόσοι άνδρες, πόσες γυναίκες και πόσα παιδιά παρευρέθηκαν;

62. (Euler, 1770) Να γράψετε το 100 ως άθροισμα δύο θετικών ακεραίων, ο ένας εκ των οποίων να διαιρείται με το 7 και ο άλλος με το 11.

63. Να λύσετε στο $\mathbb{Z}$ το ακόλουθο σύστημα εξισώσεων: $\begin{cases} 2x+5y-11z=1 \\ x-12y+7z=2 \end{cases}$

1.5 Απόδειξη του αιτήματος του Bertrand

(Αίτημα του Bertrand) Αν n είναι θετικός ακέραιος, τότε υπάρχει πρώτος p με
$$n < p \leq 2n.$$

Παρατηρούμε ότι $p = 2n$, μόνον για $n = 1$.

Ξεκινάμε την απόδειξη[2] προτάσσοντας κάποια προκαταρκτικά.

Ορισμός 1.55. Για κάθε $x \geq 0$, θέτουμε $\vartheta(x) = \sum_{p \leq x} \log p$, όπου το άθροισμα εκτείνεται για όλους **τους πρώτους p**, οι οποίοι είναι μικρότεροι ή ίσοι του x. Η συνάρτηση ϑ λέγεται **συνάρτηση του Chebyshev**. $\big($Για $x \in [0,2)$ θέτουμε $\vartheta(x) = 0\big)$.

Λήμμα 1.56. $\vartheta(n) < 2n \log 2$, για κάθε θετικό ακέραιο n.

Απόδειξη: Έστω m θετικός ακέραιος. Ο διωνυμικός συντελεστής $\binom{2m+1}{m} = \binom{2m+1}{m+1}$ εμφανίζεται δύο φορές στο άθροισμα $\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}$ και επομένως $2\binom{2m+1}{m} < 2^{2m+1} \Leftrightarrow \binom{2m+1}{m} < 2^{2m}$.

Επίσης, $\binom{2m+1}{m} = \dfrac{(2m+1)(2m)(2m-1)\cdots(m+2)}{m!}$.

Παρατηρούμε ότι όλοι οι πρώτοι p με $m+1 < p \leq 2m+1$ δεν διαιρούν τον παρονομαστή $m!$, αλλά διαιρούν τον αριθμητή $(2m+1)(2m)(2m-1)\cdots(m+2)$. Επομένως το γινόμενό τους $\prod_{m+1<p\leq 2m+1} p$ διαιρεί τον $\binom{2m+1}{m}$ και συνεπώς $\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m} < 2^{2m} \Leftrightarrow \sum_{m+1<p\leq 2m+1} \log p < 2m \log 2 \Leftrightarrow$
$\Leftrightarrow \vartheta(2m+1) - \vartheta(m+1) < 2m \log 2$.

Τώρα, το λήμμα ισχύει προφανώς για $n = 1$ και $n = 2$. Έστω ότι ισχύει για κάθε θετικό ακέραιο n, με $2 \leq n < n_0$. Θα αποδείξουμε ότι ισχύει και για το n_0. Αν το n_0 είναι περιττός της μορφής $n_0 = 2m+1$, τότε $\vartheta(n_0) = \vartheta(2m+1) - \vartheta(m+1) + \vartheta(m+1) < 2m \log 2 + \vartheta(m+1)$. Επειδή $n_0 = 2m+1 > 2 \Leftrightarrow 2m > 1 \Leftrightarrow m \geq 1 \Leftrightarrow n_0 - (m+1) \geq 1 > 0 \Leftrightarrow n_0 > m+1$, από την επαγωγική υπόθεση έχουμε $\vartheta(m+1) < 2(m+1)\log 2$. Επομένως $\vartheta(n_0) < 2m \log 2 + (2m+2)\log 2 = 2(2m+1)\log 2 = 2n_0 \log 2$.

Αν το $n_0 > 2$ είναι άρτιος, τότε ο n_0 δεν είναι πρώτος, άρα κάθε πρώτος μικρότερος ή ίσος του n_0 είναι γνήσια μικρότερος αυτού. Επομένως $\vartheta(n_0) = \sum_{p \leq n_0} \log p = \sum_{p \leq n_0 - 1} \log p = \vartheta(n_0 - 1)$. Λόγω της επαγωγικής υπόθεσης, $\vartheta(n_0 - 1) < 2(n_0 - 1)\log 2 < 2n_0 \log 2$. Η απόδειξη του λήμματος είναι πλήρης. ■

Παρατήρηση: Αν n είναι ένας θετικός ακέραιος, θεωρούμε τον διωνυμικό συντελεστή $\binom{2n}{n} = \dfrac{(2n)!}{(n!)^2}$.

Αν $\binom{2n}{n} = \prod_p p^{k_p}$ είναι η ανάλυση του $\binom{2n}{n}$ σε γινόμενο διακεκριμένων πρώτων παραγόντων (k_p η μεγαλύτερη δύναμη του πρώτου p που διαιρεί το $\binom{2n}{n}$), τότε, σύμφωνα με την πρόταση 1.19, το k_p ισούται με

[2] Η απόδειξη είναι παρμένη από το κλασικό βιβλίο των G. H. Hardy και E. M. Wright "An Introduction to the Theory of Numbers", Fifth Edition, Oxford Science Publications, 1979.

$$k_p = \sum_{i=1}^{\infty} \Big(\Big\lfloor \frac{2n}{p^i} \Big\rfloor - 2\Big\lfloor \frac{n}{p^i} \Big\rfloor \Big).$$

Παρατηρούμε ότι $\Big\lfloor \frac{n}{p^i} \Big\rfloor \le \frac{n}{p^i} < \Big\lfloor \frac{n}{p^i} \Big\rfloor + 1 \Leftrightarrow 2\Big\lfloor \frac{n}{p^i} \Big\rfloor \le \frac{2n}{p^i} < 2\Big\lfloor \frac{n}{p^i} \Big\rfloor + 2$. Επομένως $2\Big\lfloor \frac{n}{p^i} \Big\rfloor \le \Big\lfloor \frac{2n}{p^i} \Big\rfloor \le \frac{2n}{p^i} < 2\Big\lfloor \frac{n}{p^i} \Big\rfloor + 2$. Άρα $0 \le \Big\lfloor \frac{2n}{p^i} \Big\rfloor - 2\Big\lfloor \frac{2n}{p^i} \Big\rfloor < 2$. Συνεπώς ο ακέραιος $\Big\lfloor \frac{2n}{p^i} \Big\rfloor - 2\Big\lfloor \frac{2n}{p^i} \Big\rfloor$ παίρνει τις τιμές 0 ή 1. Επειδή ο $2\Big\lfloor \frac{2n}{p^i} \Big\rfloor$ είναι άρτιος, **ο ακέραιος $\Big\lfloor \frac{2n}{p^i} \Big\rfloor - 2\Big\lfloor \frac{2n}{p^i} \Big\rfloor$ δεν μηδενίζεται όταν και μόνον όταν ο $\Big\lfloor \frac{2n}{p^i} \Big\rfloor$ είναι περιττός**. Επίσης, αν $p^i > 2n$, τότε $\Big\lfloor \frac{2n}{p} \Big\rfloor = 0$ και άρα και $\Big\lfloor \frac{2n}{p^i} \Big\rfloor - 2\Big\lfloor \frac{2n}{p^i} \Big\rfloor = 0$. Άρα $p^i \le 2n \Leftrightarrow i \log p \le \log(2n) \Leftrightarrow i \le \dfrac{\log(2n)}{\log p}$. Εφόσον, για κάθε i προσθέτουμε 1 ή 0 στο k_p,

η μέγιστη τιμή που μπορεί να πάρει το k_p είναι λοιπόν $\Big\lfloor \dfrac{\log(2n)}{\log p} \Big\rfloor$ (1).

Απόδειξη της εικασίας του Bertrand: Υποθέτουμε ότι μπορούμε να βρούμε n, οσονδήποτε μεγάλο, ώστε η εικασία του Bertrand να μην ισχύει για τον n. Μπορούμε να υποθέσουμε ότι $n \ge 5$. Στο διάστημα λοιπόν $(n, 2n)$ δεν περιέχεται κανένας πρώτος αριθμός. Θεωρούμε τον διωνυμικό συντελεστή $N = \binom{2n}{n}$. Οι πιθανοί πρώτοι διαιρέτες του, οι οποίοι είναι και διαιρέτες του $(2n)!$ $\big($άρα βρίσκονται στο σύνολο $\{1, 2, \ldots, 2n\}\big)$ θα πρέπει αναγκαστικά, εφόσον δεν ισχύει η εικασία του Bertrand για τον n, να είναι μικρότεροι ή ίσοι του n. Αν p είναι ένας τέτοιος πρώτος, τότε διακρίνουμε δύο πιθανές περιπτώσεις:

1) $\frac{2}{3}n < p \le n$. Τότε $2p \le 2n < 3p \Leftrightarrow 2 \le \dfrac{2n}{p} < 3$. Επομένως $\Big\lfloor \dfrac{2n}{p} \Big\rfloor = 2$. Σύμφωνα με την προηγούμενη παρατήρηση, θα έχουμε $\Big\lfloor \dfrac{2n}{p} \Big\rfloor - 2\Big\lfloor \dfrac{2n}{p} \Big\rfloor = 0$. Επίσης, $p^2 > \frac{4}{9}n^2 > 2n$. (Η ανισότητα $\frac{4}{9}n^2 > 2n$ προκύπτει από την υπόθεση $n \ge 5$). Άρα $\dfrac{2n}{p^2} < 1$ και συνεπώς $\dfrac{2n}{p^i} < 1$, για κάθε $i \ge 2$. Επομένως $\Big\lfloor \dfrac{2n}{p^i} \Big\rfloor = 0$. Με βάση πάλι την προηγούμενη παρατήρηση, θα έχουμε πάλι $\Big\lfloor \dfrac{2n}{p^i} \Big\rfloor - 2\Big\lfloor \dfrac{2n}{p^i} \Big\rfloor = 0$, για κάθε $i \ge 2$. Συνεπώς $k_p = 0$, δηλαδή ο p δεν είναι διαιρέτης του N και η περίπτωση $\frac{2}{3}n < p \le n$ αποκλείεται.

2) Από το 1) απομένουν μόνον οι πρώτοι p που είναι μικρότεροι ή ίσοι του $\frac{2}{3}n$.

Αν $k_p \ge 2$, τότε $2\log p \le k_p \log p \underset{\text{σχέση (1)}}{\le} \dfrac{\log(2n)}{\log p} \log p = \log(2n)$. Άρα $\log p \le \log(\sqrt{2n}) \Leftrightarrow p \le \sqrt{2n}$. Υπάρχουν λοιπόν το πολύ $\sqrt{2n}$ τέτοιοι p. Συνεπώς $\sum\limits_{k_p \ge 2} k_p \log p \le \sqrt{2n}\log(2n)$.

Επομένως $\log N = \sum\limits_{k_p = 1} \log p + \sum\limits_{k_p \ge 2} k_p \log p \le \sum\limits_{p \le \frac{2}{3}n} \log p + \sqrt{2n}\log(2n) = \vartheta\big(\frac{2}{3}n\big) + \sqrt{2n}\log(2n) \underset{\text{Λήμμα 1.56}}{\le}$
$\le \frac{4}{3}n\log 2 + \sqrt{2n}\log(2n)$.

Από την άλλη μεριά, ο διωνυμικός συντελεστής $N = \binom{2n}{n}$ είναι ο μεγαλύτερος συντελεστής στο άθροισμα

$$2^{2n} = \binom{2n}{0} + \binom{2n}{1} + \binom{2n}{2} + \cdots + \binom{2n}{2n-1} + \binom{2n}{2n} = \underbrace{2 + \binom{2n}{1} + \binom{2n}{2} + \cdots + \binom{2n}{2n-1}}_{2n \text{ όροι}}.$$

$\Big($Προφανώς $2 = \binom{2}{1} < \binom{2n}{1} < \binom{2n}{n} = N\Big)$. Άρα $2^{2n} < 2nN \Leftrightarrow 2n\log 2 < \log(2n) + \log N$.

Συνεπώς $2n\log 2 < \log(2n) + \frac{4}{3}n\log 2 + \sqrt{2n}\log(2n) \Leftrightarrow 2n\log 2 < 3(1+\sqrt{2n})\log(2n)$.

Βρίσκουμε τώρα ένα $\zeta > 0$ τέτοιο, ώστε $2n = 2^{10(1+\zeta)} \Leftrightarrow \log(2n) = 10(1+\zeta)\log 2 \Leftrightarrow \zeta = \dfrac{\log(n/2^5)}{10\log 2}$. Αν $n > 2^5 = 512$, τότε $\zeta = \dfrac{\log(n/2^5)}{10\log 2} > 0$. Στην περίπτωση αυτή η σχέση $2n\log 2 < 3(1+\sqrt{2n})\log(2n)$ γίνεται

$2^{10(1+\zeta)}\log 2 < 3(1+\sqrt{2^{10(1+\zeta)}})\log 2^{10(1+\zeta)} \Leftrightarrow 2^{10(1+\zeta)}\log 2 < 30(1+2^{5(1+\zeta)})(1+\zeta)\log 2 \Leftrightarrow 2^{10(1+\zeta)} < 30(1+2^{5(1+\zeta)})(1+\zeta) \Leftrightarrow 2^{5\zeta} < 30\cdot 2^{-10-5\zeta}(1+2^{5(1+\zeta)})(1+\zeta) = 30\cdot 2^{-5}(2^{-5(1+\zeta)}+1)(1+\zeta) < 30\cdot 2^{-5}(2^{-5}+1)(1+\zeta)$. Αλλά $30\cdot 2^{-5} < 1-2^{-5} \Leftrightarrow \dfrac{31}{32} < 1$. Επομένως $2^{5\zeta} < (1-2^{-5})(1+2^{-5})(1+\zeta) = (1-2^{-10})(1+\zeta) < 1+\zeta$. Αλλά $2^{5\zeta} = e^{\log(2^{5\zeta})} = e^{\zeta\log(32)} > 1+\zeta\log 32 \underset{32>e}{>} 1+\zeta$, αντίφαση. Συνεπώς, για $n > 512$ η εικασία του Bertrand ισχύει.

Τώρα, θεωρούμε τους πρώτους 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631. Καθένας από αυτούς είναι μικρότερος από το διπλάσιο του προηγουμένου του. Άρα αν το n είναι κάποιος από αυτούς, τότε ανάμεσα στο n και το $2n$ υπάρχει πρώτος. Αν τώρα το n βρίσκεται ανάμεσα σε δύο διαδοχικούς τέτοιους πρώτους, δηλαδή $p_1 < n < p_2$, όπου p_1, p_2 κάποιος από τους προηγούμενους πρώτους, τότε $n < p_2 < 2p_1 < 2n$, δηλαδή ο p_2 είναι ανάμεσα στο n και το $2n$. Συνεπώς η εικασία του Bertrand ισχύει και για κάθε θετικό ακέραιο μικρότερο ή ίσο του $512 < 631$. (Για $n > 512$ η εικασία του Bertrand έχει αποδειχθεί προηγουμένως). ■

1.6 Λύσεις των ασκήσεων του κεφαλαίου 1

1. Όχι. Ο αριθμός 6^7 είναι άρτιος και δεν μπορεί να γραφεί ως άθροισμα περιττού πλήθους περιττών.

2. Επειδή έχουμε τρεις ακεραίους, δύο από αυτούς αναγκαστικά θα είναι και οι δύο άρτιοι ή και οι δύο περιττοί. Σε κάθε περίπτωση το άθροισμά τους είναι άρτιο.

3. $\beta < 0$ γιατί $35\beta = -313 - \upsilon$, άρα $|\beta| = -\beta$. $313 = 35|\beta| - \upsilon \leq 35|\beta| \Leftrightarrow 8 + \frac{33}{35} \leq |\beta|$. Αλλά $313 = 35|\beta| - \upsilon > 34|\beta| \Leftrightarrow |\beta| < 9 + \frac{7}{34}$. Άρα $|\beta| = 9 \Leftrightarrow \beta = -9$ και συνεπώς $\upsilon = 2$.

4. Έστω $\alpha = (\alpha - \beta)\pi_1 + \upsilon_1$ και $\beta = (\alpha - \beta)\pi_2 + \upsilon_2$ με $0 \leq \upsilon_1, \upsilon_2 < |\alpha - \beta|$. Τότε $\alpha - \beta = (\alpha - \beta)(\pi_1 - \pi_2) + \upsilon_1 - \upsilon_2 \Rightarrow \alpha - \beta \mid \upsilon_1 - \upsilon_2$. Επειδή $0 \leq |\upsilon_1 - \upsilon_2| < |\alpha - \beta|$, $\upsilon_1 - \upsilon_2 = 0$.

5. Από τη διαίρεση $\gamma : 12$ προκύπτει ότι $0 < 3\beta < 12 \Leftrightarrow 0 < \beta < 4$. Αλλά από τη διαίρεση $\alpha : \beta$, $\beta > 2$. Άρα $\beta = 3$, $\alpha = 3 \cdot 7 + 2 = 23$, $\gamma = 12 \cdot 23 + 9 = 285$.

6. $n(7n^2+5) = 6n^3 + n(n^2+5) = 6n^3 + 6n + n(n^2-1) = 6n(n^2+1) + (n-1)n(n+1)$ και $6 = 3! \mid (n-1)n(n+1)$.

7. **(i)** $5^2 + 7 = 32 = 4 \cdot 8$. Έστω $8 \mid 5^{2n} + 7 = 8\lambda$. Τότε $5^{2n+2} + 7 = 25 \cdot 5^{2n} + 7 = 24 \cdot 5^{2n} + 8\lambda = 8 \cdot (3 \cdot 5^{2n} + \lambda)$.
(ii) $2^4 - 1 = 15$. Έστω $15 \mid 2^{4n} - 1 = 15\lambda$. Τότε $2^{4n+4} - 1 = 16 \cdot 2^{4n} - 1 = 15 \cdot 2^{4n} + 2^{4n} - 1 = 15(2^{4n} + \lambda)$.
(iii) $3^4 + 2^2 = 81 + 4 = 85 = 5 \cdot 17$. Έστω $5 \mid 3^{3n+1} + 2^{n+1} = 5\lambda$. Τότε $3^{3n+4} + 2^{n+2} = 27 \cdot 3^{3n+1} + 2 \cdot 2^{n+1} = 25 \cdot 3^{3n+1} + 2(3^{3n+1} + 2^{n+1}) = 5(5 \cdot 3^{3n+1} + 2\lambda)$.
(iv) $4^2 + 5^1 = 21$. Έστω $21 \mid 4^{n+1} + 5^{2n-1} = 21\lambda$. Τότε $4^{n+2} + 5^{2n+1} = 4 \cdot 4^{n+1} + 25 \cdot 5^{2n-1} = 21 \cdot 5^{2n-1} + 4(4^{n+1} + 5^{2n-1}) = 21(5^{2n-1} + \lambda)$.
(v) $2 \cdot 7 + 3 \cdot 5 - 5 = 24$. Έστω $24 \mid 2 \cdot 7^n + 3 \cdot 5^n - 5 = 24\lambda$. Τότε $2 \cdot 7^{n+1} + 3 \cdot 5^{n+1} - 5 - 24\lambda = 14 \cdot 7^n + 15 \cdot 5^n - 5 - (2 \cdot 7^n + 3 \cdot 5^n - 5) = 12(7^n + 5^n)$. Ο $7^n + 5^n$ είναι άρτιος ως άθροισμα δύο περιττών. Άρα $7^n + 5^n = 2\rho$ και άρα $2 \cdot 7^{n+1} + 3 \cdot 5^{n+1} - 5 = 24(\lambda + \rho)$.

8. Έστω $\alpha = \pi\beta + \upsilon$, $0 \leq \upsilon < |\beta|$ η ταυτότητα της ευκλείδειας διαίρεσης $\alpha : \beta$. Αν $\upsilon \leq \frac{1}{2}|\beta|$, τότε θέτουμε $q = \pi$ και $r = \upsilon$. Αν $\frac{1}{2}|\beta| < \upsilon < |\beta|$, τότε $\alpha = \pi\beta + |\beta| + \upsilon - |\beta|$. Αν $\epsilon = \begin{cases} 1, & \text{αν } \beta > 0 \\ -1, & \text{αν } \beta < 0 \end{cases}$ το πρόσημο του β, τότε θέτουμε $q = \pi + \epsilon$ και $r = \upsilon - |\beta|$. Προφανώς $\alpha = q\beta + r$. Επίσης $-\frac{1}{2}|\beta| < r = \upsilon - |\beta| < 0$. Αν $\alpha = q'\beta + r'$, για κάποια άλλα $q', r' \in \mathbb{Z}$ με $-\frac{1}{2}|\beta| < r' \leq \frac{1}{2}|\beta|$, τότε $|\beta||q - q'| = |r - r'|$. Αν $q \neq q'$, τότε $|r - r'| \geq |\beta|$. Αλλά $-\frac{1}{2}|\beta| < r \leq \frac{1}{2}|\beta|$ (1) και $-\frac{1}{2}|\beta| < r' \leq \frac{1}{2}|\beta| \Leftrightarrow -\frac{1}{2}|\beta| \leq -r' < \frac{1}{2}|\beta|$ (2). Προσθέτοντας τις (1) και (2) παίρνουμε $-|\beta| < r - r' < |\beta| \Leftrightarrow |r - r'| < |\beta|$, αντίφαση. Άρα $q = q'$ και συνεπώς $r = r'$.

9. Έστω $x = 2\alpha + 3\beta$ και $y = 9\alpha + 5\beta$. Το αποτέλεσμα προκύπτει από τις σχέσεις $4x + y = 17(\alpha + \beta)$ και $x - 4y = -17(2\alpha + \beta)$.

10. **(i)** Το άθροισμα των τετραγώνων δύο περιττών είναι άρτιος. Αν αυτό ήταν τετράγωνο, θα ήταν τετράγωνο αρτίου, δηλαδή της μορφής $4\rho^2$. Από το (ii) του παραδείγματος 1.4 το τετράγωνο περιττού είναι της μορφής $8\lambda + 1$. Άρα θα είχαμε $4\rho^2 = 8\lambda + 1 + 8\lambda' + 1 \Rightarrow 2\rho^2 = 4(\lambda + \lambda') + 1 \Rightarrow 2 \mid 1$, άτοπο.
(ii) $n(n+1)(n+2)(n+3) = n^4 + 6n^3 + 11n^2 + 6n = (n^2 + 3n + 1)^2 - 1$.

11. Ο αριθμός $8n + 5$ είναι περιττός και αν διαιρεθεί με το 8 δίνει υπόλοιπο 5. Το αποτέλεσμα προκύπτει από το (ii) του παραδείγματος 1.4.

12. Προφανώς για $n = 2$ παίρνουμε $2^n + 5 = 2^2 + 5 = 9 = 3^2$. Αν $n > 2$, τότε $8 \mid 2^n$ και άρα το αποτέλεσμα προκύπτει ξανά από το (ii) του παραδείγματος 1.4.

13. **(i)** $n^2 + 2 = n^2 + 2n + 2 - 2n = n(n+2) - 2(n-1) = n(n+2) - 2(n+2) + 6$. Άρα $n + 2 \mid 6 \underset{n+2 \geq 3}{\Leftrightarrow} n + 2 = 3$ ή $n + 2 = 6$. Άρα $n = 1$ ή $n = 4$.
(ii) $2n - 1 \mid n^2 - n - 1 \Rightarrow 2n - 1 \mid 2n^2 - 2n - 2 = n(2n-1) - (n+2)$. Άρα $2n-1 \mid n+2 \Rightarrow 2n-1 \mid 2(n+2) = 2n + 4 = 2n - 1 + 5$. Άρα $2n - 1 \mid 5 \Leftrightarrow 2n - 1 = 1$ ή $5 \Leftrightarrow n = 1$ ή $n = 3$. Επαλήθευση: $2 \cdot 1 - 1 = 1 \mid -1 = 1^2 - 1 - 1$ και $2 \cdot 3 - 1 = 5 \mid 5 = 3^2 - 3 - 1$.

14. Έστω $\alpha = 2k + 1$. $\alpha^2 + (\alpha+2)^2 + (\alpha+4)^2 + 1 = 3(\alpha^2 + 7) + 12\alpha$. Αρκεί $4 \mid \alpha^2 + 7$. $\alpha^2 + 7 = (2k+1)^2 + 7 = 4(k^2 + k + 2)$.

15. Έστω $\mathrm{A}_n = 1 + 7 + 7^2 + \cdots + 7^{4n-1}$. $\mathrm{A}_1 = 1 + 7 + 7^2 + 7^3 = 8 + 7^2(1+7) = 8(1 + 7^2) = 8 \cdot 50 = 400$. Υποθέτουμε ότι $400 \mid \mathrm{A}_n = 400\lambda$. Τότε $\mathrm{A}_{n+1} = \mathrm{A}_n + 7^{4n} + 7^{4n+1} + 7^{4n+2} + 7^{4n+3} = 400\lambda + 7^{4n} \cdot (1 + 7 + 7^2 + 7^3) = 400\lambda + 7^{4n} \cdot \mathrm{A}_1 = 400\lambda + 7^{4n} \cdot 400 = 400(\lambda + 7^{4n})$.

16. **(i)** $n(n^2+11) = n(n^2+12-1) = 12n + (n-1)n(n+1)$. Προφανώς $6 \mid 12n$ και $6 = 3! \mid (n-1)n(n+1)$. (Άσκηση 1.12).
(ii) Έστω $n = 2k + 1$. $n(n^2 - 1) = (n-1)n(n+1) = 2k(2k+1)(2k+2) = 4k(k+1)(2k+1) = 4k(k+1)(3 + 2k - 2) = 12k(k+1) + 8(k-1)k(k+1)$. $2 \mid k(k+1) \Rightarrow 24 \mid 12k(k+1)$, $6 = 3! \mid (k-1)k(k+1) \Rightarrow 24 \mid 48 \mid 8(k-1)k(k+1)$.
(iii) Από το (ii) του παραδείγματος 1.4, $m^2 = 8\lambda + 1$, $n^2 = 8\lambda' + 1$, άρα $m^2 - n^2 = 8(\lambda - \lambda')$.
(iv) $m^2 + 23 = 24 + (m-1)(m+1)$. Αρκεί να δείξουμε ότι $24 \mid (m-1)(m+1)$. Αν διαιρέσουμε το m με το 6 θα πάρουμε $m = 6k$ ή $m = 6k + 1$ ή $m = 6k + 2$ ή $m = 6k + 3$ ή $m = 6k + 4$ ή $m = 6k + 5$. Οι περιπτώσεις $m = 6k$, $m = 6k + 2$, $m = 6k + 3$ και $m = 6k + 4$ αποκλείονται γιατί $2, 3 \nmid m$. Επομένως $m = 6k + 1$ ή

$m = 6k+5$. Αν $m = 6k+1$, τότε $(m-1)(m+1) = 6k(6k+2) = 12k(3k+1) = 12k(2k+(k+1)) = 24k^2+12k(k+1)$ και ο $k(k+1)$ άρτιος. Αν $m = 6k+5$, τότε $(m-1)(m+1) = (6k+4)6(k+1) = 12(3k+2)(k+1) = 12(k+2(k+1))(k+1) = 12k(k+1)+24(k+1)^2$ και $k(k+1)$ άρτιος.
(v) $m^2(m^2-1)(m^2-4) = (m-2)(m-1)m(m+1)(m+2)m$ και $120 = 5! \mid (m-2)(m-1)m(m+1)(m+2)$, άρα $120 \mid (m-2)(m-1)m(m+1)(m+2)m$. Επομένως $m^2(m^2-1)(m^2-4) = 120\lambda$. Πρέπει να δείξουμε ότι $360 \mid 120\lambda \Leftrightarrow 3 \mid \lambda$. Αν $3 \mid m$, τότε $9 \mid m^2$. Αν $m = 3k+1$, τότε $9 \mid (m-1)(m+2) = 3k(3k+3)$. Αν $m = 3k+2$, τότε $9 \mid (m-2)(m+1) = 3k(3k+3)$. Σε κάθε περίπτωση $9 \mid 120\lambda \Leftrightarrow 3 \mid 40\lambda = 39\lambda+\lambda = 3\cdot 13\lambda+\lambda$. Άρα $3 \mid \lambda$.

17. Αν $1 = \frac{1}{k_1}+\frac{1}{k_2}+\cdots+\frac{1}{k_n}$, τότε $k_1k_2\cdots k_n = k_2k_3\cdots k_n + k_1k_3\cdots k_n + \cdots k_1\cdots k_{i-1}k_{i+1}\cdots k_n + \cdots + k_1k_2\cdots k_{n-1}$. Στο πρώτο μέλος έχουμε γινόμενο περιττών, άρα περιττό. Στο δεύτερο μέλος έχουμε άρτιο (n) άθροισμα περιττών γινομένων, άρα άρτιο. Άτοπο.

18. Μπορούμε να βρούμε ακριβώς n. Το $S = \{n+1, n+2, \ldots, 2n\}$ έχει αυτή την ιδιότητα. Πράγματι, αν $n+1 \le \alpha < \beta \le 2n$ και $\alpha \mid \beta$, τότε αν $\beta = \lambda\alpha$, θα έπρεπε $\lambda \ge 2$, γιατί $\beta > \alpha$. Επομένως θα είχαμε $\beta \ge 2\alpha \ge 2(n+1) > 2n$, άτοπο.

19. $\delta = (x,y) \Rightarrow \delta \mid \alpha x+\beta y = 1 \Leftrightarrow \delta = 1$.

20. Αληθεύει. Αν $\delta = (r,s)$, τότε $\delta \mid s+t$ και $\delta \mid s$, άρα $\delta \mid t$. Επομένως $\delta \mid (s,t) = 1$. Ομοίως $(r,t) = 1$.

21. $227 = 143+84$, $143 = 84+59$, $84 = 59+25$, $59 = 2\cdot 25+9$, $25 = 2\cdot 9+7$, $9 = 7+2$, $7 = 3\cdot 2+1$. Άρα $(227,143) = 1$. $657 = 2\cdot 306+45$, $306 = 6\cdot 45+36$, $45 = 36+9$, $36 = 4\cdot 9$. Άρα $(306,657) = 9$. $1479 = 5\cdot 272+119$, $272 = 2\cdot 119+34$, $119 = 3\cdot 34+17$, $34 = 2\cdot 17$. Άρα $(272,1479) = 17$.

22. **(i)** $72 = 56+16$, $56 = 3\cdot 16+8$, $16 = 2\cdot 8$. Άρα $8 = (56,72) = 56-3\cdot 16 = 56-3\cdot(72-56) = 4\cdot 56+(-3)72$.
(ii) $138 = 5\cdot 24+18$, $24 = 18+6$, $18 = 3\cdot 6$. Άρα $6 = (24,138) = 24-18 = 24-(138-5\cdot 24) = 6\cdot 24+(-1)138$.
(iii) $651 = 395+256$, $395 = 256+139$, $256 = 139+117$, $139 = 117+22$, $117 = 5\cdot 22+7$, $22 = 3\cdot 7+1$. Άρα $1 = (651,395) = 22-3\cdot 7 = 22-3(117-5\cdot 22) = 6\cdot 22+(-3)117 = 6(139-117)+(-3)117 = 6\cdot 139+(-9)117 = 6\cdot 139+(-9)(256-139) = 15\cdot 139+(-9)256 = 15(395-256)+(-9)256 = 15\cdot 395+(-24)256 = 15\cdot 395+(-24)(651-395) = (-24)651+39\cdot 395$.
(iv) $2378 = 1769+609$, $1769 = 2\cdot 609+551$, $609 = 551+58$, $551 = 9\cdot 58+29$, $58 = 2\cdot 29$. Άρα $29 = (1769,-2378) = (1769,2378) = 551-9\cdot 58 = 551-9(609-551) = 10\cdot 551+(-9)609 = 10(1769-2\cdot 609)+(-9)609 = 10\cdot 1769+(-29)609 = 10\cdot 1769+(-29)(2378-1769) = 39\cdot 1769+29\cdot(-2378)$.

23. **(i)** Έστω $\delta = (2\alpha+\beta, \alpha+2\beta)$. Τότε $\delta \mid 2\alpha+\beta-2(\alpha+2\beta) = -3\beta$. Ομοίως, $\delta \mid \alpha+2\beta-2(2\alpha+\beta) = -3\alpha$. Επομένως $\delta \mid (-3\alpha,-3\beta) = 3(\alpha,\beta) = 3$. Άρα $\delta = 1$ ή 3.
(ii) $(\alpha+\beta,\alpha^2+\beta^2) = (\alpha+\beta,(\alpha+\beta)^2-2\alpha\beta) = (\alpha+\beta,-2\alpha\beta) \mid (\alpha+\beta,2)(\alpha+\beta,\alpha)(\alpha+\beta,\beta) = (\alpha+\beta,2)(\alpha,\beta)^2 = (\alpha+\beta,2) \mid 2$. Άρα $(\alpha+\beta,\alpha^2+\beta^2) = 1$ ή 2.
(iii) $(\alpha+\beta,\alpha^2-\alpha\beta+\beta^2) = (\alpha+\beta,(\alpha+\beta)^2-3\alpha\beta) = (\alpha+\beta,-3\alpha\beta) \mid (\alpha+\beta,3)(\alpha+\beta,\alpha)(\alpha+\beta,\beta) = (\alpha+\beta,3)(\alpha,\beta)^2 = (\alpha+\beta,3) \mid 3$. Άρα $(\alpha+\beta,\alpha^2-\alpha\beta+\beta^2) = 1$ ή 3.
(iv) $(\alpha^2-\beta^2,2\alpha\beta) \mid (\alpha^2-\beta^2,2)(\alpha^2-\beta^2,\alpha)(\alpha^2-\beta^2,\beta)$. Έστω $\delta = (\alpha^2-\beta^2,\alpha)$. Τότε $\delta \mid \alpha$, άρα $\delta \mid \alpha^2$. Επειδή $\delta \mid \alpha^2-\beta^2$, έχουμε $\delta \mid \beta^2$. Επομένως $\delta \mid (\alpha^2,\beta^2) = (\alpha,\beta)^2 = 1$. Ομοίως αποδεικνύουμε ότι $(\alpha^2-\beta^2,\beta) = 1$. Άρα $(\alpha^2-\beta^2,2\alpha\beta) \mid (\alpha^2-\beta^2,2) \mid 2$.

24. Αν κάποιος από τους m,n διαιρεί τον άλλο, π.χ. $m \mid n$, τότε και τα δύο μέλη θα είναι ίσα με α^n-1. Έστω $[\alpha^m-1,\alpha^n-1] = \alpha^{[m,n]}-1$. Έστω $m > n$, $\delta = (m,n)$, $m = x\delta$ και $n = y\delta$ με $(x,y) = 1$ και $x > y$. Τότε $[\alpha^m-1,\alpha^n-1] = \alpha^{[m,n]}-1 \Leftrightarrow \frac{(\alpha^{x\delta}-1)(\alpha^{y\delta}-1)}{\alpha^\delta-1} = \alpha^{xy\delta}-1 \Leftrightarrow \alpha^{(x+y)\delta}-\alpha^{x\delta}-\alpha^{y\delta}+1 = \alpha^{(xy+1)\delta}-\alpha^{xy\delta}-\alpha^\delta+1 \Leftrightarrow \alpha^{xy\delta}-1 \Leftrightarrow \alpha^{(x+y)\delta}-\alpha^{x\delta}-\alpha^{y\delta} = \alpha^{(xy+1)\delta}-\alpha^{xy\delta}-\alpha^\delta$. Έστω $\beta = \alpha^\delta > 1$. Τότε $\beta^{x+y}-\beta^x-\beta^y = \beta^{xy+1}-\beta^{xy}-\beta$. Αν $y > 1$, τότε $\beta^{x+y-1}-\beta^{x-1}-\beta^{y-1} = \beta^{xy}-\beta^{xy-1}-1$ και επομένως $\beta \mid 1$, άτοπο γιατί $\beta > 1$. Άρα $y = 1$, $n = y\delta = \delta \mid x\delta = m$. Ομοίως, αν $n > m$, τότε $m \mid n$. Η περίπτωση $m = n$ είναι τετριμμένη.

25. $(\alpha,\beta) = [\alpha,\beta] \Leftrightarrow \left[\frac{\alpha}{(\alpha,\beta)},\frac{\beta}{(\alpha,\beta)}\right] = 1 \Leftrightarrow \frac{|\alpha|}{(\alpha,\beta)}\frac{|\beta|}{(\alpha,\beta)} = 1 \Leftrightarrow \frac{|\alpha|}{(\alpha,\beta)} = \frac{|\beta|}{(\alpha,\beta)} = 1 \Leftrightarrow |\alpha| = |\beta| = (\alpha,\beta) \Leftrightarrow \alpha = \pm\beta$.

26. **(i)** $147 = 5\cdot 28+7$, $28 = 4\cdot 7$. Άρα $(147,28) = 7$ και $7 = 147+(-5)28$. $7 = 6+1$, άρα $(7,6) = 1$ και $1 = (147,28,6) = 7+(-1)6 = 147+(-5)28+(-1)6$.
(ii) $288 = 198+90$, $198 = 2\cdot 90+18$, $90 = 5\cdot 18$. Άρα $(198,288) = 18 = 198-2\cdot 90 = 198-2(288-198) = 3\cdot 198+(-2)288$. Επίσης $512 = 28\cdot 18+8$, $18 = 2\cdot 8+2$, $8 = 4\cdot 2$. Επομένως $2 = (198,288,512) = 18-2\cdot 8 = 18-2(512-28\cdot 18) = 57\cdot 18+(-2)512 = 57(3\cdot 198+(-2)288)+(-2)512 = 171\cdot 198+(-114)288+(-2)512$.

27. Ο παρονομαστής μηδενίζεται για $\kappa = -\frac{3}{2} \notin \mathbb{Z}$, άρα για κάθε $\kappa \in \mathbb{Z}$ το κλάσμα ορίζεται. Έστω $\delta = (\kappa^2+3\kappa+2, 2\kappa+3)$. Τότε $\delta \mid 2(\kappa^2+3\kappa+2) = 2\kappa^2+6\kappa+4$ και $\delta \mid \kappa(2\kappa+3) = 2\kappa^2+3\kappa$. Επομένως $\delta \mid 2\kappa^2+6\kappa+4-(2\kappa^2+3\kappa) = 3\kappa+4$. Επίσης $\delta \mid 3(2\kappa+3) = 6\kappa+9$ και $\delta \mid 2(3\kappa+4) = 6\kappa+8$. Επομένως $\delta \mid 6\kappa+9-(6\kappa+8) = 1$.

28. Προφανώς $(f_1,f_2) = (1,1) = 1$. Έστω $(f_n,f_{n+1}) = 1$. Τότε $(f_{n+1},f_{n+2}) = (f_{n+1},f_{n+1}+f_n) = (f_{n+1},f_n) = 1$.

29. Έστω $\delta = (n!+1,(n+1)!+1)$. Τότε $\delta \mid (n+1)(n!+1) = (n+1)!+n+1$. Επομένως $\delta \mid (n+1)!+n+1-((n+1)!+1) = n \Rightarrow \delta \mid n!$ Εφόσον $\delta \mid n!+1$, $\delta \mid n!+1-n! = 1$.

30. $\frac{r}{s}+\frac{u}{v}=\frac{rv+su}{sv}\in\mathbb{Z}\Leftrightarrow sv\mid rv+su$. $s\mid su$, άρα $s\mid rv\underset{(s,r)=1}{\Leftrightarrow}s\mid v$. Ομοίως $v\mid rv$, άρα $v\mid su\underset{(v,u)=1}{\Leftrightarrow}v\mid s$.

31. Έστω $\delta=(5k-4,9k-7)$. Τότε $\delta\mid 45k-36$ και $\delta\mid 45k-35$. Επομένως $\delta\mid 45k-36-(45k-35)=-1\Leftrightarrow\delta=1$.

32. $\pm1=\alpha\beta'-\alpha'\beta=\alpha\beta'+\alpha'\beta'-\alpha'\beta'-\alpha'\beta=(\alpha+\alpha')\beta'-\alpha'(\beta+\beta')$, οπότε $(\alpha+\alpha',\beta+\beta')\mid\pm1$, δηλαδή $(\alpha+\alpha',\beta+\beta')=1$.

33. Έστω $\alpha=x(\alpha,\beta)$ και $\beta=y(\alpha,\beta)$. Αν διαιρέσουμε την αποδεικτέα σχέση με (α,β), θα πάρουμε την ισοδύναμη $(x+y,[x,y])=1\underset{(x,y)=1}{\Leftrightarrow}(x+y,xy)=1$. Έχουμε $(x+y,xy)\underset{(x,y)=1}{=}(x+y,x)(x+y,y)=(x,y)^2=1$.

34. Έστω $x=\frac{\alpha}{(\alpha,\beta)}$ και $y=\frac{\beta}{(\alpha,\beta)}$. Τότε $(x,y)=1$ και $xy=[x,y]=\left[\frac{\alpha}{(\alpha,\beta)},\frac{\beta}{(\alpha,\beta)}\right]=\frac{[\alpha,\beta]}{(\alpha,\beta)}=\frac{420}{12}=35=5\cdot7$. Εφόσον $12=(\alpha,\beta)<20<\alpha<\beta$, $x=\frac{\alpha}{(\alpha,\beta)}>\frac{20}{12}>1$ και $y>x$. Οι μόνοι διαιρέτες του 35, όπως με δοκιμή μπορούμε να δούμε είναι το 1, το 5, το 7 και το 35. Επομένως $x=5$ και $y=7$. Άρα $\alpha=5\cdot12=60$ και $\beta=7\cdot12=84$.

35. Υπάρχουν $\kappa,\lambda\in\mathbb{Z}$ με $\kappa\alpha+\lambda\beta=1$. Επομένως $x=x^1=x^{\kappa\alpha+\lambda\beta}=(x^\alpha)^\kappa\cdot(x^\beta)^\lambda=(y^\beta)^\kappa\cdot(x^\beta)^\lambda=(y^\kappa x^\lambda)^\beta$. Επομένως ο αριθμός $\sqrt[\beta]{x}=y^\kappa x^\lambda\in\mathbb{Q}$, άρα $\sqrt[\beta]{x}\in\mathbb{Z}$. Έστω $n=\sqrt[\beta]{x}$. Τότε $n^\beta=x$ και άρα $y^\beta=(n^\beta)^\alpha=(n^\alpha)^\beta$. Επομένως $y=n^\alpha$.

36. $(x,y)\mid[x,y]$ και $(x,y)\mid x+y$. Επομένως $(x,y)\mid-1\Leftrightarrow(x,y)=1\Rightarrow[x,y]=xy$. Άρα $x+y-1=xy\Leftrightarrow(x-1)(y-1)=0$. Εφόσον $y\le x$, $y=1$ και x οποιοσδήποτε θετικός ακέραιος.

37. Διαιρούμε το $(\alpha\kappa,\beta\lambda)$ με $(\alpha,\beta)(\kappa,\lambda)\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)$ και παίρνουμε $\left(\frac{\frac{\alpha}{(\alpha,\beta)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\cdot\frac{\kappa}{(\kappa,\lambda)},\frac{\beta}{(\alpha,\beta)}\cdot\frac{\frac{\lambda}{(\kappa,\lambda)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\right)$.
Τώρα $\frac{\frac{\alpha}{(\alpha,\beta)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\ \Big|\ \frac{\alpha}{(\alpha,\beta)}$ και $\left(\frac{\alpha}{(\alpha,\beta)},\frac{\beta}{(\alpha,\beta)}\right)=1$.
Άρα $\left(\frac{\frac{\alpha}{(\alpha,\beta)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)},\frac{\beta}{(\alpha,\beta)}\right)=1$.
Επίσης $\left(\frac{\frac{\alpha}{(\alpha,\beta)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)},\frac{\frac{\lambda}{(\kappa,\lambda)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\right)=1$. Επομένως $\left(\frac{\frac{\alpha}{(\alpha,\beta)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)},\frac{\beta}{(\alpha,\beta)}\cdot\frac{\frac{\lambda}{(\kappa,\lambda)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\right)=1$ και κατά συνέπεια $\left(\frac{\frac{\alpha}{(\alpha,\beta)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\cdot\frac{\kappa}{(\kappa,\lambda)},\frac{\beta}{(\alpha,\beta)}\cdot\frac{\frac{\lambda}{(\kappa,\lambda)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\right)=$
$=\left(\frac{\kappa}{(\kappa,\lambda)},\frac{\beta}{(\alpha,\beta)}\cdot\frac{\frac{\lambda}{(\kappa,\lambda)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\right)$. Επίσης $\frac{\frac{\lambda}{(\kappa,\lambda)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\ \Big|\ \frac{\lambda}{(\kappa,\lambda)}$ και $\left(\frac{\kappa}{(\kappa,\lambda)},\frac{\lambda}{(\kappa,\lambda)}\right)=1$. Άρα $\left(\frac{\kappa}{(\kappa,\lambda)},\frac{\frac{\lambda}{(\kappa,\lambda)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\right)=1$. Επομένως $\left(\frac{\kappa}{(\kappa,\lambda)},\frac{\beta}{(\alpha,\beta)}\cdot\frac{\frac{\lambda}{(\kappa,\lambda)}}{\left(\frac{\alpha}{(\alpha,\beta)},\frac{\lambda}{(\kappa,\lambda)}\right)}\right)=\left(\frac{\kappa}{(\kappa,\lambda)},\frac{\beta}{(\alpha,\beta)}\right)$.

38. Έστω $x=p_1^{r_1}p_2^{r_2}\cdots p_n^{r_n}$ και $y=p_1^{s_1}p_2^{s_2}\cdots p_n^{s_n}$, όπου p_i διαφορετικοί πρώτοι και $r_i,s_i\ge0$. Τότε $x^\alpha=y^\beta\Leftrightarrow p_1^{\alpha r_1}p_2^{\alpha r_2}\cdots p_n^{\alpha r_n}=p_1^{\beta s_1}p_2^{\beta s_2}\cdots p_n^{\beta s_n}\Leftrightarrow\alpha r_i=\beta s_i$, για κάθε $i=1,\dots,n$. Εφόσον $\alpha\mid\beta s_i$ και $(\alpha,\beta)=1$, $\alpha\mid s_i=\lambda_i\alpha$. Επομένως $\alpha r_i=\lambda_i\beta\alpha\Leftrightarrow r_i=\lambda_i\beta$. Έστω $n=p_1^{\lambda_1}p_2^{\lambda_2}\cdots p_n^{\lambda_n}$. Τότε $n^\alpha=p_1^{\alpha\lambda_1}p_2^{\alpha\lambda_2}\cdots p_n^{\alpha\lambda_n}=$ $=p_1^{s_1}p_2^{s_2}\cdots p_n^{s_n}=y$ και $n^\beta=p_1^{\beta\lambda_1}p_2^{\beta\lambda_2}\cdots p_n^{\beta\lambda_n}=$ $=p_1^{r_1}p_2^{r_2}\cdots p_n^{r_n}=x$.

39. $79860=2^2\cdot3\cdot5\cdot11^3$, $4851=3^2\cdot7^2\cdot11$, $20475=3^2\cdot5^2\cdot7\cdot13$. Επομένως $(79860,4851,20475)=3$ και $[79860,4851,20475]=2^2\cdot3^2\cdot5^2\cdot7^2\cdot11^3\cdot13=763062300$.

40. **(i)** Το 2 είναι της μορφής (για $n=0$) $3n+2$. Άρα ένας πρώτος της μορφής $3n+1$ είναι περιττός. Τότε ο n είναι άρτιος, γιατί σε αντίθετη περίπτωση ο $3n$ θα ήταν περιττός και επομένως ο $3n+1$ άρτιος. Άρα $n=2k$ και κατά συνέπεια ο αριθμός είναι της μορφής $6k+1$.
(ii) Το 3 δεν διαιρεί τον ακέραιο αυτό, γιατί τότε ο ακέραιος θα ήταν της μορφής $3n$. Άρα οι πρώτοι διαιρέτες του $3n+2$ είναι της μορφής $3k+1$ ή $3k+2$. Επειδή το γινόμενο αριθμών της μορφής $3k+1$ είναι πάλι της ίδιας μορφής $\big((3k+1)(3r+1)=3(3kr+k+r)+1\big)$, αριθμός θα πρέπει να έχει έναν πρώτο διαιρέτη της μορφής $3k+2$.
(iii) $n^3-1=(n-1)(n^2+n+1)$. Αν $n>2$, τότε $n-1>1$ και ο n^3-1 θα ήταν σύνθετος. Επομένως $n=2$ και $n^3-1=2^3-1=7$.
(iv) Έστω $3p+1=x^2\Leftrightarrow3p=(x-1)(x+1)$. Αν $x-1=1\Leftrightarrow x=2$, τότε $x+1=3$ και άρα $p=1$, άτοπο. Επομένως $3=x-1$ και $p=x+1$. Συνεπώς $3=x-1\Leftrightarrow x=4$ και $p=4+1=5$.
(v) $n^2-4=(n-2)(n+2)$. Επειδή ο $(n-2)(n+2)$ είναι πρώτος, θα πρέπει $n-2=1\Leftrightarrow n=3$. Συνεπώς $n^2-4=3^2-4=5$.

41. Εφόσον $p\ge5$, $p\ne3$. Άρα $p=3k+1$ ή $p=3k+2$. Τότε $p^2+2=(3k+1)^2+2=3(3k^2+2k+1)$ ή $p^2+2=(3k+2)^2+2=3(3k^2+4k+2)$, δηλαδή $3\mid p^2+2$ και άρα ο p^2+2 είναι σύνθετος.

42. $n^4+4=n^4+4n^2+4-4n^2=(n^2+2)^2-(2n)^2=(n^2-2n+2)(n^2+2n+2)$ και $n^2-2n+2=n(n-2)+2\ge2$. Άρα ο n^4+4 είναι σύνθετος.

43. $k!\mid p(p-1)\cdots(p-k+1)$. Επειδή p πρώτος και $1<k<p$, $(k!,p)=1$. Επομένως $k!\mid(p-1)\cdots(p-k+1)=\lambda k!$, όπου $\lambda\in\mathbb{Z}$. Άρα $\binom{p}{k}=\frac{p(p-1)\cdots(p-k+1)}{k!}=p\lambda$.

44. Οι πρώτοι παράγοντες του 50! είναι όλοι οι πρώτοι που είναι μικρότεροι του 50. Αυτοί είναι: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47. Βρίσκουμε τους εκθέτες: $\left\lfloor\frac{50}{2}\right\rfloor+\left\lfloor\frac{50}{4}\right\rfloor+\left\lfloor\frac{50}{8}\right\rfloor+\left\lfloor\frac{50}{16}\right\rfloor+\left\lfloor\frac{50}{32}\right\rfloor=25+12+6+3+1=47$, $\left\lfloor\frac{50}{3}\right\rfloor+\left\lfloor\frac{50}{9}\right\rfloor+\left\lfloor\frac{50}{27}\right\rfloor=16+5+1=22$, $\left\lfloor\frac{50}{5}\right\rfloor+\left\lfloor\frac{50}{25}\right\rfloor=10+2=12$, $\left\lfloor\frac{50}{7}\right\rfloor+\left\lfloor\frac{50}{49}\right\rfloor=7+1=8$, $\left\lfloor\frac{50}{11}\right\rfloor=4$, $\left\lfloor\frac{50}{13}\right\rfloor=3$, $\left\lfloor\frac{50}{17}\right\rfloor=2$, $\left\lfloor\frac{50}{19}\right\rfloor=2$, $\left\lfloor\frac{50}{23}\right\rfloor=2$,

$\lfloor\frac{50}{29}\rfloor = \lfloor\frac{50}{31}\rfloor = \lfloor\frac{50}{37}\rfloor = \lfloor\frac{50}{41}\rfloor = \lfloor\frac{50}{43}\rfloor = \lfloor\frac{50}{47}\rfloor = 1$. Επομένως $50! = 2^{47}\cdot 3^{22}\cdot 5^{12}\cdot 7^8\cdot 11^4\cdot 13^3\cdot 17^2\cdot 19^2\cdot 23^2\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47$.

45. $\lfloor\sqrt{353}\rfloor = 18$. Κανείς από τους 2, 3, 5, 7, 11, 13, 17 δεν διαιρεί τον 353, άρα αυτός είναι πρώτος. $\lfloor\sqrt{379}\rfloor = 19$. Πιθανοί πρώτοι διαιρέτες: 2, 3, 5, 7, 11, 13, 17, 19. Κανείς δεν διαιρεί τον 379, άρα αυτός είναι πρώτος. $\lfloor\sqrt{403}\rfloor = 20$. Πιθανοί πρώτοι διαιρέτες: 2, 3, 5, 7, 11, 13, 17, 19. $403 = 13\cdot 31$, άρα 403 σύνθετος. $\lfloor\sqrt{439}\rfloor = 20$. Πιθανοί πρώτοι διαιρέτες: 2, 3, 5, 7, 11, 13, 17, 19. Κανείς δεν τον διαιρεί, άρα 439 πρώτος. $\lfloor\sqrt{451}\rfloor = 21$. Πιθανοί πρώτοι διαιρέτες: 2, 3, 5, 7, 11, 13, 17, 19. $451 = 11\cdot 41$, άρα 451 σύνθετος. $\lfloor\sqrt{499}\rfloor = 22$. Πιθανοί πρώτοι διαιρέτες: 2, 3, 5, 7, 11, 13, 17, 19. Κανείς δεν τον διαιρεί, άρα 499 πρώτος. $\lfloor\sqrt{769}\rfloor = 27$. Πιθανοί πρώτοι διαιρέτες: 2, 3, 5, 7, 11, 13, 17, 19, 23. Κανείς δεν τον διαιρεί, άρα 769 πρώτος. $\lfloor\sqrt{899}\rfloor = 29$. Πιθανοί πρώτοι διαιρέτες: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. $899 = 29\cdot 31$, άρα 899 σύνθετος.

46. $\binom{1325}{660} = \frac{1325!}{660!\cdot 665!}$. Επειδή $21 = 3\cdot 7$ και $\lfloor\frac{n}{3^i}\rfloor \geq \lfloor\frac{n}{7^i}\rfloor$, αρκεί να υπολογίσουμε τη μεγαλύτερη δύναμη του 7 που διαιρεί τα 1325!, 660! και 665!. Έχουμε $\lfloor\frac{1325}{7}\rfloor + \lfloor\frac{1325}{49}\rfloor + \lfloor\frac{1325}{343}\rfloor = 189+27+3 = 219$, $\lfloor\frac{660}{7}\rfloor + \lfloor\frac{660}{49}\rfloor + \lfloor\frac{660}{343}\rfloor = 94+13+1 = 108$ και $\lfloor\frac{665}{7}\rfloor + \lfloor\frac{665}{49}\rfloor + \lfloor\frac{665}{343}\rfloor = 95+13+1 = 109$. Άρα η μεγαλύτερη δύναμη του 21 που διαιρεί τον $\binom{1325}{660}$ έχει εκθέτη $219-108-109 = 2$, δηλαδή είναι το 21^2.

47. **(i)** $31p = x^2-1 = (x-1)(x+1)$. Αν $31 = x-1$, τότε $p = x+1 = 33 = 3\cdot 11$, άτοπο. Επομένως $31 = x+1$ και $p = x-1 = 29$.
(ii) $23p = x^2-4 = (x-2)(x+2)$. Αν $23 = x-2$, τότε $p = x+2 = 27 = 3^3$, άτοπο. Επομένως $23 = x+2$ και $p = x-2 = 19$.
(iii) Αν $p = 2$, τότε $8p+9 = 16+9 = 25 = 5^2$. Έστω p περιττός. Τότε $8p = x^2-9 = (x-3)(x+3)$, για κάποιον περιττό x. Οι $x-3$ και $x+3$ είναι άρτιοι. Επομένως $2p = \frac{x-3}{2}\cdot\frac{x+3}{2}$. Επομένως $2 = \frac{x-3}{2} \Leftrightarrow x = 7$ και $p = \frac{x+3}{2} = 5$. Πράγματι, $8\cdot 5+9 = 49 = 7^2$.
(iv) Αν $p = 2$, τότε $5p+16 = 26$, που δεν είναι τέλειο τετράγωνο. Άρα p περιττός και συνεπώς και ο $5p+16$ είναι περιττός. Τότε $5p = x^2-16 = (x-4)(x+4)$, για κάποιον περιττό x. Έστω $5 = x-4 \Leftrightarrow x = 9$. Τότε $p = 9+4 = 13$. Πράγματι, $5\cdot 13+16 = 81 = 9^2$. Αν $5 = x+4$, τότε $x = 1$, άτοπο.

48. **(i)** Αν $p = q$, τότε προφανώς $24 \mid 0 = p^2-q^2$. Έστω $p > q \geq 5$. Επειδή $3 \nmid p, q$, οι αριθμοί αυτοί θα είναι της μορφής $3k+1$ ή $3k+2$. Αν είναι της ίδιας μορφής, τότε $3 \mid p-q$. Αν είναι διαφορετικής μορφής, τότε $3 \mid p+q$. Σε κάθε περίπτωση $3 \mid p^2-q^2 = (p-q)(p+q)$. Τώρα, και οι δύο είναι περιττοί. Άρα τα τετράγωνά τους είναι της μορφής $8\lambda+1$. (Παράδειγμα 1.4 (ii)). Επομένως $8 \mid p^2-q^2$. Εφόσον $(3,8) = 1$, έχουμε $3\cdot 8 = 24 \mid p^2-q^2$.
(ii) Κατ' αρχάς και οι δύο αριθμοί p^2-1, p^2+1 είναι άρτιοι. Αρκεί να δείξουμε ότι κάποιος διαιρείται με το 5. Από το παράδειγμα 1.4 (iv) προκύπτει ότι οι πιθανές μορφές για το p^2 είναι $5k+1$ ή $5k+4$. Στην πρώτη περίπτωση $5 \mid p^2-1$, ενώ στη δεύτερη $5 \mid p^2+1$.

49. Αν p είναι ένας πρώτος διαιρέτης του N, τότε $p = p_i$, για κάποιο $i = 1, 2, \ldots, n$. Αλλά τότε ο $p = p_i$ θα διαιρούσε όλους τους όρους του N εκτός από τον $p_1\cdots p_{i-1}p_{i+1}\cdots p_n$. Κατά συνέπεια $p \nmid$ N, αντίφαση.

50. Αν ο q ήταν περιττός, τότε ο $p = q+3 > 2$ θα ήταν άρτιος. Επομένως ο q είναι άρτιος, δηλαδή $q = 2$ και $p = 5$.

51. **(i)** Ο πέμπτος όρος της ακολουθίας των πρώτων είναι ο $11 > 2\cdot 5-1$. Υποθέτουμε ότι για κάποιο $n \geq 5$ ισχύει $p_n > 2n-1$. Προφανώς $p_{n+1} \geq p_n+2 > 2n-1+2 = 2(n+1)-1$.
(ii) Επειδή $p_1 = 2$, ο P_n είναι περιττός. Αν ήταν τετράγωνο, θα ήταν τετράγωνο κάποιου περιττού x, δηλαδή $p_1p_2\cdots p_n = (x-1)(x+1)$. Οι $x\pm 1$ είναι άρτιοι, άρα $4 \mid 2p_2\cdots p_n \Leftrightarrow 2 \mid p_2\cdots p_n$, άτοπο γιατί όλοι οι πρώτοι μεγαλύτεροι του 2 είναι περιττοί.
(iii) Το άθροισμα $\frac{1}{p_1}+\frac{1}{p_2}+\cdots+\frac{1}{p_n}$ ισούται με $\frac{\text{N}}{p_1p_2\cdots p_n}$, όπου N ο ακέραιος της άσκησης 49. Αλλά όπως είδαμε, κανείς από τους $p_1, p_2, \ldots, p_n$ δεν διαιρεί τον N.

52. Έστω α και β οι ζητούμενοι ακέραιοι. Τότε, σύμφωνα με την άσκηση 33, $(\alpha,\beta) = (\alpha+\beta, [\alpha,\beta]) = (27, 60) = (3^3, 2^2\cdot 3\cdot 5) = 3$. Επομένως $\alpha\beta = (\alpha,\beta)[\alpha,\beta] = 3\cdot 60 = 180$. Οι α, β είναι οι ρίζες της εξίσωσης $t^2-27t+180 = 0 \Leftrightarrow t = \begin{cases}\frac{27+3}{2} = 15\\ \frac{27-3}{2} = 12\end{cases}$

53. $p > q$. Μια προφανής λύση είναι $p = 5$ και $q = 3$. Θα δείξουμε ότι είναι και η μοναδική. $p+q = p^3-3p^2q+3pq^2-q^3$. Άρα $q \mid p^3-p = p(p-1)(p+1)$. Εφόσον $p \neq q$, $q \mid (p-1)(p+1)$. Έστω $q \mid p-1 \Leftrightarrow p = \lambda q+1$, $\lambda \geq 2$. (Αν $p = q+1$, τότε αναγκαστικά $q = 2$ και $p = 3$, άτοπο). $p+q = 1+(\lambda+1)q$, $p-q = 1+(\lambda-1)q$. Άρα $1+(\lambda+1)q = ((\lambda-1)q+1)^3 = (\lambda-1)^3q^3+3(\lambda-1)^2q^2+3(\lambda-1)q+1 \Leftrightarrow \lambda-1 = (\lambda-1)^3q^2+3(\lambda-1)^2q+3(\lambda-1)-2 \underset{\lambda>1}{>} (\lambda-1)^3q^2+3(\lambda-1)^2q+3(\lambda-1) > 3(\lambda-1) \Rightarrow \lambda < 1$, άτοπο. Επομένως $q \mid p+1 \Leftrightarrow p = \lambda q-1$, $\lambda > 1$. Άρα $p+q = (\lambda+1)q-1$ και $p-q = (\lambda-1)q-1$. Άρα $(\lambda+1)q-1 = ((\lambda-1)q-1)^3 = (\lambda-1)^3q^3-3(\lambda-1)^2q^2+3(\lambda-1)q-1 \Leftrightarrow \lambda+1 = (\lambda-1)^3q^2-3(\lambda-1)^2q+3(\lambda-1) \Leftrightarrow \lambda-1 = (\lambda-1)^3q^2-3(\lambda-1)^2q+3(\lambda-1)-2 \Rightarrow \lambda-1 \mid 2$. Αν $\lambda-1 = 1 \Leftrightarrow \lambda = 2$, τότε $q^2-3q = 0 \Leftrightarrow q(q-3) = 0$ και άρα $q = 3$ και $p = 5$, αποδεκτή λύση. Αν $\lambda-1 = 2 \Leftrightarrow \lambda = 3$, τότε $2 = 8q^2-12q+4 \Leftrightarrow 4q^2-6q+1 = 0$, με διακρίνουσα $\Delta = 20$, που δεν είναι τέλειο τετράγωνο, άρα q άρρητος. Μοναδική λύση: $q = 3$ και $p = 5$.

54. **(i)** $72 = 56 + 16$, $56 = 3 \cdot 16 + 8$, $16 = 2 \cdot 8$. Άρα $8 = 56 - 3 \cdot 16 = 56 - 3(72 - 56) = 4 \cdot 56 + (-3) \cdot 72$. Επομένως $56 \cdot 20 + 72(-15) = 40$. $x = 20 - \frac{72}{8} \cdot t = 20 - 9t$, $y = -15 + \frac{56}{8} \cdot t = -15 + 7t$, $t \in \mathbb{Z}$.
(ii) $138 = 5 \cdot 24 + 18$, $24 = 18 + 6$, $18 = 3 \cdot 6$. Άρα $6 = 24 - 18 = 24 - (138 - 5 \cdot 24) = 24 \cdot 6 + 138 \cdot (-1)$. Επομένως $24 \cdot 18 + 138(-3) = 18$. $x = 18 - \frac{138}{6} \cdot t = 18 - 23t$, $y = -3 + \frac{24}{6} \cdot t = -3 + 4t$, $t \in \mathbb{Z}$.
(iii) $221 = 6 \cdot 35 + 11$, $35 = 3 \cdot 11 + 2$, $11 = 5 \cdot 2 + 1$. Άρα $1 = 11 - 5 \cdot 2 = 11 - 5(35 - 3 \cdot 11) = 11 \cdot 16 + 35 \cdot (-5) = (221 - 6 \cdot 35) \cdot 16 + 35 \cdot (-5) = 221 \cdot 16 + 35 \cdot (-101)$. Επομένως $221 \cdot 16 \cdot 11 + 35 \cdot (-101) \cdot 11 = 11 \Leftrightarrow 221 \cdot 176 + 35 \cdot (-1111) = 11$. $x = 176 - 35t$, $y = -1111 + 221t$, $t \in \mathbb{Z}$.

55. **(i)** $18 = 3 \cdot 5 + 3$, $5 = 3 + 2$, $3 = 2 + 1$. Άρα $1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2(18 - 3 \cdot 5) - 5 = 2 \cdot 18 - 7 \cdot 5$. Επομένως $18 \cdot 2 \cdot 48 + 5(-7 \cdot 48) = 48 \Leftrightarrow 18 \cdot 96 + 5(-336) = 48$. Άρα $x = 96 - 5t$ και $y = -336 + 18t$, $t \in \mathbb{Z}$. Θα πρέπει $96 - 5t > 0 \Leftrightarrow t < \frac{96}{5} = 19 + \frac{1}{5}$. Άρα $t \leq 19$. Επίσης $-336 + 18t > 0 \Leftrightarrow t > \frac{336}{18} = 18 + \frac{2}{3} \Leftrightarrow t \geq 19$. Επομένως $t = 19$, $x = 96 - 5 \cdot 19 = 1$, $y = -336 + 18 \cdot 19 = 6$.
(ii) $54 = 2 \cdot 21 + 12$, $21 = 12 + 9$, $12 = 9 + 3$. Άρα $3 = 12 - 9 = 12 - (21 - 12) = 2 \cdot 12 - 21 = 2(54 - 2 \cdot 21) - 21 = 54 \cdot 2 + 21(-5)$. Επομένως $54 \cdot 2 \cdot 302 + 21(-5 \cdot 302) = 906 \Leftrightarrow 54 \cdot 604 + 21(-1510) = 906$. Άρα $x = 604 - 7t$ και $y = -1510 + 18t$, $t \in \mathbb{Z}$. Θα πρέπει $604 - 7t > 0 \Leftrightarrow t < \frac{604}{7} = 86 + \frac{2}{7}$. Άρα $t \leq 86$. Επίσης $-1510 + 18t > 0 \Leftrightarrow t > \frac{1510}{18} = 83 + \frac{8}{9} \Leftrightarrow t \geq 84$. Επομένως $t = 84$ ή 85 ή 86. Για $t = 84$ παίρνουμε $x = 604 - 7 \cdot 84 = 16$ και $y = -1510 + 18 \cdot 84 = 2$. Για $t = 85$ παίρνουμε $x = 604 - 7 \cdot 85 = 9$ και $y = -1510 + 18 \cdot 85 = 20$. Τέλος, για $t = 86$ παίρνουμε $x = 604 - 7 \cdot 86 = 2$ και $y = -1510 + 18 \cdot 86 = 38$.
(iii) Η εξίσωση αυτή δεν έχει θετικές λύσεις γιατί, για κάθε ζεύγος (x, y) θετικών ακεραίων έχουμε $123x + 360y \geq 123 + 360 = 483 > 99$.
(iv) $158 = 2 \cdot 57 + 44$, $57 = 44 + 13$, $44 = 3 \cdot 13 + 5$, $13 = 2 \cdot 5 + 3$, $5 = 3 + 2$ και $3 = 2 + 1$. Επομένως $1 = 3 - 2 = 3 - (5 - 3) = (-1)5 + 2 \cdot 3 = (-1)5 + 2(13 - 2 \cdot 5) = 2 \cdot 13 + (-5)5 = 2 \cdot 13 + (-5)(44 - 3 \cdot 13) = 17 \cdot 13 + (-5)44 = 17(57 - 44) + (-5)44 = 17 \cdot 57 + (-22)44 = 17 \cdot 57 + (-22)(158 - 2 \cdot 57) = 158(-22) + 57 \cdot 61$. Άρα $158(-22 \cdot 7) + 57 \cdot 61 \cdot 7 = 7 \Leftrightarrow 158(-154) + 57 \cdot 427 = 7 \Leftrightarrow 158(-154) + (-57)(-427) = 7$. Η γενική λύση της $158x - 57y = 7$ δίνεται από τον τύπο $(x, y) = (-154 + 57t, -427 + 158t)$, $t \in \mathbb{Z}$. Θα πρέπει $57t > 154 \Leftrightarrow t > \frac{154}{57} = 2 + \frac{40}{57} \Leftrightarrow t \geq 3$. Επίσης $158t > 427 \Leftrightarrow t > \frac{427}{158} = 2 + \frac{111}{158} \Leftrightarrow t \geq 3$. Οι θετικές λύσεις δίνονται απ' τον τύπο $(x, y) = (-154 + 57t, -427 + 158t)$, $t = 3, 4, \ldots$ ή ισοδύναμα $(x, y) = (17 + 57t, 47 + 158t)$, $t = 0, 1, 2, \ldots$

56. $21 = 3 \cdot 7$, $14 = 2 \cdot 7$ και $6 = 2 \cdot 3$. Άρα $(21, 14, 6) = 1$ και $(21, 14) = 7$. $7 + 6(-1) = 1 \Leftrightarrow 7 \cdot 74 + 6(-74) = 74$. Επίσης $21 + 14(-1) = 7$. Η γενική λύση της εξίσωσης $21x + 14y + 6z = 74$ δίνεται από τους τύπους:
$$\begin{cases} x = 74 - 6t - 2s \\ y = -74 + 6t + 3s \quad t, s \in \mathbb{Z}. \\ z = -74 + 7t \end{cases}$$
Πρέπει $z = -74 + 7t > 0 \Leftrightarrow t > \frac{74}{7} = 10 + \frac{4}{7} \Leftrightarrow t \geq 11$. $x > 0 \Leftrightarrow 74 - 6t > 2s \Leftrightarrow s < 37 - 3t$ και $y > 0 \Leftrightarrow 3s > 74 - 6t \Leftrightarrow s > \frac{74-6t}{3}$. Επομένως $\frac{74-6t}{3} < s < 37 - 3t \Rightarrow 74 - 6t < 111 - 9t \Leftrightarrow t < \frac{37}{3} = 12 + \frac{1}{3}$. Άρα $t \leq 12$. Για $t = 11$ παίρνουμε $2 + \frac{2}{3} < s < 4 \Leftrightarrow s = 3$. Επομένως
$$\begin{cases} x = 74 - 66 - 6 = 2 \\ y = -74 + 66 + 9 = 1 \\ z = -74 + 77 = 3 \end{cases}$$
Για $t = 12$ παίρνουμε $\frac{2}{3} < s < 1$, αδύνατον γιατί $s \in \mathbb{Z}$.

57. Εφόσον $(\alpha, \beta) = 1 \mid \gamma$, η εξίσωση $\alpha x - \beta y = \gamma$ έχει λύσεις. Έστω (x_0, y_0) μια λύση αυτής. Τότε όλες οι λύσεις δίνονται από τον τύπο $(x, y) = (x_0 + \beta t, y_0 + \alpha t)$, όπου $t \in \mathbb{Z}$. Πρέπει $x > 0 \Leftrightarrow \beta t > -x_0 \Leftrightarrow t > -\frac{x_0}{\beta}$ και $y > 0 \Leftrightarrow \alpha t > -y_0 \Leftrightarrow t > -\frac{y_0}{\alpha}$. Έστω $A = \max\{-\frac{x_0}{\beta}, -\frac{y_0}{\alpha}\} \in \mathbb{R}$. Επειδή το σύνολο των ακεραίων δεν είναι άνω φραγμένο, υπάρχουν άπειροι ακέραιοι $t > A$, άρα και άπειρες θετικές λύσεις της εξίσωσης $\alpha x - \beta y = \gamma$.

58. Έστω x οι σοκολάτες και y οι καραμέλες. Τότε $2,5x + 0,3y = 13,5 \Leftrightarrow 25x + 3y = 135$. Έχουμε $25 = 8 \cdot 3 + 1 \Leftrightarrow 25 + 3(-8) = 1 \Leftrightarrow 25 \cdot 135 + 3(-8 \cdot 135) = 135 \Leftrightarrow 25 \cdot 135 + 3(-1080) = 135$. Η γενική λύση της εξίσωσης $25x + 3y = 135$ είναι λοιπόν $(x, y) = (135 - 3t, -1080 + 25t)$, όπου $t \in \mathbb{Z}$. Θα πρέπει $x > 0 \Leftrightarrow 135 > 3t \Leftrightarrow t < 45 \Leftrightarrow t \leq 44$. Επίσης $y > 0 \Leftrightarrow 25t > 1080 \Leftrightarrow 5t > 216 \Leftrightarrow t > \frac{216}{5} = 43 + \frac{1}{5} \Leftrightarrow t \geq 44$. Επομένως $t = 44$, $x = 135 - 3 \cdot 44 = 3$ και $y = -1080 + 25 \cdot 44 = 20$.

59. Έστω x τα πρόβατα και y τα γίδια. Τότε $65x + 40y = 1040 \Leftrightarrow 13x + 8y = 208$. Έχουμε $13 = 8 + 5$, $8 = 5 + 3$, $5 = 3 + 2$ και $3 = 2 + 1$. Επομένως $1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 + (-1)5 = 2 \cdot (8 - 5) + (-1)5 = 2 \cdot 8 + (-3)5 = 2 \cdot 8 + (-3)(13 - 8) = 13(-3) + 8 \cdot 5$. Επομένως $13(-3 \cdot 208) + 8 \cdot 5 \cdot 208 = 208 \Leftrightarrow 13(-624) + 8 \cdot 1040 = 208$. Η γενική λύση της $13x + 8y = 208$ είναι $(x, y) = (-624 - 8t, 1040 + 13t)$, όπου $t \in \mathbb{Z}$. Πρέπει $x > 0 \Leftrightarrow t < -78 \Leftrightarrow 7 \leq -79$ και $13t > -1040 \Leftrightarrow t > -80 \Leftrightarrow t \geq -79$. Επομένως $t = -79$, $x = -624 - 8(-79) = 8$ και $y = 1040 + 13(-79) = 13$.

60. Έστω $\delta = (9k - 7, 5k + 4)$. Τότε $\delta \mid 45k - 35$ και $\delta \mid 45k + 36$. Επομένως $\delta \mid 36 + 35 = 71$. Επειδή το 71 είναι πρώτος, $\delta = 1$ ή $\delta = 71$. Επομένως θα πρέπει $9k - 7 = 71\lambda$ και $5k + 4 = 71\mu$, όπου $\lambda, \mu \in \mathbb{Z}$. Λύνουμε τις γραμμικές εξισώσεις $9k - 71\lambda = 7$ και $5k - 71\mu = -4$. Έχουμε $71 = 7 \cdot 9 + 8$ και $9 = 8 + 1$. Άρα $1 = 9 - 8 = 9 - (71 - 7 \cdot 9) = 9 \cdot 8 + 71(-1) = 1 \Leftrightarrow$

$9\cdot 56+(-71)\cdot 7=7$. Η γενική λύση της $9k-71\lambda=7$ είναι $(k,\lambda)=(56+71t,7+9t)$, $t\in\mathbb{Z}$. Επίσης $71=14\cdot 5+1 \Leftrightarrow 5(-14)+71=1 \Leftrightarrow 5\cdot 56+(-71)\cdot 4=-4$. Η γενική λύση της $5k-71\mu=-4$ είναι $(k,\mu)=(56+71s,4+5s)$, $s\in\mathbb{Z}$. Θα πρέπει $56+71t=56+71s \Leftrightarrow t=s$. Επομένως $k=56+71t$, $t\in\mathbb{Z}$. Τότε $9k-7=497+639t=71(7+9t)$ και $5k+4=284+355t=71(4+5t)$. Τότε $\delta=71\delta'$, όπου $\delta'=(7+9t,4+5t)$. Αλλά $\delta'\mid 5(7+9t)=35+45t$ και $\delta'\mid 9(4+5t)=36+45t$. Επομένως $\delta'\mid 36+45t-35-45t=1\Rightarrow \delta'=1\Leftrightarrow \delta=71$.

61. x άντρες, y γυναίκες και $z=20-x-y$ παιδιά. Τότε $3x+2y+\frac{1}{2}(20-x-y)=20 \Leftrightarrow 5x+3y=20$. $5=3+2$, $3=2+1$, άρα $1=(5,3)=3-2=3-(5-3)=5(-1)+3\cdot 2$. Άρα $5(-20)+3\cdot 40=20$. Επομένως $(x,y)=(-20-3t,40+5t)$, όπου $t\in\mathbb{Z}$. Έχουμε $x>0 \Leftrightarrow -20-3t>0 \Leftrightarrow t<-\frac{20}{3}=-6-\frac{2}{3} \Leftrightarrow t\le -7$, $y>0 \Leftrightarrow t>-8 \Leftrightarrow t\ge -7$. Άρα $t=-7$, $x=1$, $y=5$ και $z=20-1-5=14$.

62. Έστω $100=7x+11y$, όπου $x,y>0$. Έχουμε $11=7+4$, $7=4+3$ και $4=3+1$. Επομένως $1=4-3=4-(7-4)=2\cdot 4+(-1)7=2(11-7)+(-1)7=11\cdot 2+7(-3)$. Επομένως $7(-300)+11\cdot 200=100$. Συνεπώς $x=-300-11t$ και $y=200+7t$, όπου $t\in\mathbb{Z}$. Πρέπει $x>0 \Leftrightarrow t<-\frac{300}{11}=-27-\frac{3}{11} \Leftrightarrow t\le -28$. Επίσης $y>0\Leftrightarrow t>-\frac{200}{7}=-28-\frac{4}{7}\Leftrightarrow t\ge -28$. Άρα $t=-28$, $x=-300-11(-28)=8$ και $y=200+7(-28)=4$. Οι ζητούμενοι αριθμοί είναι λοιπόν $7\cdot 8=56$ και $11\cdot 4=44$.

63. Λύνουμε το σύστημα ως προς x και y και παίρνουμε
$$\begin{cases} x=\frac{22+97z}{29} \\ y=\frac{25z-3}{29}\end{cases} \Leftrightarrow \begin{cases} 29x-97z=22 \\ -29y+25z=3\end{cases}$$
Κατά τα γνωστά, η $29x-97z=22$ έχει γενική λύση $(x,z)=(-220+97t,-66+29t)$, $t\in\mathbb{Z}$ και η $-29y+25z=3$ έχει γενική λύση $(y,z)=(18-25s,21-29s)$, $s\in\mathbb{Z}$. Εξισώνουμε τις δύο εκφράσεις για το z και παίρνουμε $-66+29t=21-29s \Leftrightarrow s+t=3 \Leftrightarrow s=3-t$. Αντικαθιστούμε το $s=3-t$ στο y και παίρνουμε $y=-57+25t$. Οι λύσεις του συστήματος δίνονται λοιπόν απ' τον τύπο:
$$\begin{cases} x=-220+97t \\ y=-57+25t \\ z=-66+29t\end{cases} ,t\in\mathbb{Z}$$

Κεφάλαιο 2

Ισοτιμίες και αριθμητικές συναρτήσεις

2.1 Ορισμοί-βασικές ιδιότητες

Ορισμός 2.1. Έστω n θετικός ακέραιος. Αν $\alpha, \beta \in \mathbb{Z}$, τότε λέμε ότι **ο α είναι ισοδύναμος (ή ισότιμος) με τον β modulo n αν και μόνον αν $n \mid \alpha - \beta$**. Στην περίπτωση αυτή γράφουμε $\alpha \underset{\mod n}{\equiv} \beta$ ή συνηθέστερα $\alpha \equiv \beta \mod n$.

Πόρισμα 2.2. $\alpha \equiv 0 \mod n \Leftrightarrow n \mid \alpha$. ■

Παράδειγμα 2.3. **(i)** $27 \equiv -8 \mod 5$, γιατί $5 \mid 35 = 27 - (-8)$.
(ii) $3227 \equiv 4 \mod 11$, γιατί $11 \mid 3227 - 4 = 3223 = 11 \cdot 293$.
(iii) $-156 \equiv 5 \mod 7$, γιατί $-156 - 5 = -161 = -23 \cdot 7 \equiv 0 \mod 7$. (Βλέπε προηγούμενο πόρισμα).

Πρόταση 2.4. Η σχέση $(\equiv \mod n)$ είναι σχέση ισοδυναμίας στο σύνολο $\mathbb{Z}$ των ακεραίων αριθμών.
Απόδειξη: (Ανακλαστική) Προφανώς $n \mid \alpha - \alpha = 0 \Leftrightarrow \alpha \equiv \alpha \mod n$, για κάθε $\alpha \in \mathbb{Z}$.
(Συμμετρική) $\alpha \equiv \beta \mod n \Leftrightarrow n \mid \alpha - \beta \Leftrightarrow n \mid \beta - \alpha = -(\alpha - \beta) \Leftrightarrow \beta \equiv \alpha \mod n$.
(Μεταβατική) Έστω $\alpha \equiv \beta \mod n$ και $\beta \equiv \gamma \mod n$. Τότε $n \mid \alpha - \beta$ και $n \mid \beta - \gamma$. Άρα $n \mid (\alpha - \beta) + (\beta - \gamma) = \alpha - \gamma \Rightarrow \alpha \equiv \gamma \mod n$. ■

Ορισμός 2.5. Η σχέση ισοδυναμίας $(\equiv \mod n)$ λέγεται **ισοτιμία (modulo n)**.

Πρόταση 2.6. Δύο ακέραιοι α, β είναι ισοδύναμοι modulo n αν και μόνον αν **τα υπόλοιπα των διαιρέσεων $\alpha : n$ και $\beta : n$ είναι ίσα**. Γι' αυτό πολλές φορές δύο αριθμοί, οι οποίοι είναι ισοδύναμοι modulo n λέγονται και **ισοϋπόλοιποι** modulo n.
Απόδειξη: Κατ' αρχάς, κάθε ακέραιος είναι ισοδύναμος modulo n με το υπόλοιπο της διαίρεσής του με το n. Πράγματι, έστω $\alpha = n\pi + \upsilon$ η ταυτότητα της ευκλειδείου διαιρέσεως $\alpha : n$. Τότε $n \mid n\pi = \alpha - \upsilon \Rightarrow \alpha \equiv \upsilon \mod n$.
Τώρα, τα δυνατά υπόλοιπα της διαίρεσης ενός ακεραίου με το n είναι $0, 1, 2, \ldots, n-1$. Αρκεί να δείξουμε ότι $\upsilon \not\equiv \upsilon' \mod n$, για κάθε $\upsilon, \upsilon' \in \{0, 1, \ldots, n-1\}$ με $\upsilon \neq \upsilon'$.
Έστω λοιπόν $\upsilon, \upsilon' \in \{0, 1, \ldots, n-1\}$. Έχουμε $0 \leq \upsilon < n$ (1) και $0 \leq \upsilon' < n \Leftrightarrow -n < -\upsilon' \leq 0$ (2). Αν προσθέσουμε κατά μέλη τις (1) και (2) θα πάρουμε $-n < \upsilon - \upsilon' < n \Leftrightarrow 0 \leq |\upsilon - \upsilon'| < n$. Αν λοιπόν $\upsilon \equiv \upsilon' \mod n \Leftrightarrow n \mid \upsilon - \upsilon'$, τότε $\upsilon - \upsilon' = \lambda n$, για κάποιο $\lambda \in \mathbb{Z}$. Κατά συνέπεια $|\upsilon - \upsilon'| = |\lambda| n$. Αν $\lambda \neq 0$, τότε $|\lambda| \geq 1$ και συνεπώς $|\upsilon - \upsilon'| \geq n$, άτοπο. Άρα $\lambda = 0 \Leftrightarrow \upsilon = \upsilon'$. ■

Πρόταση 2.7. Δύο αριθμοί α και β είναι ισοϋπόλοιποι modulo n αν και μόνον αν διαφέρουν κατά ακέραιο πολλαπλάσιο του n.
Απόδειξη: $\alpha \equiv \beta \mod n \Leftrightarrow n \mid \alpha - \beta \Leftrightarrow \alpha - \beta = \lambda n$, $\lambda \in \mathbb{Z} \Leftrightarrow \alpha = \beta + \lambda n \Leftrightarrow \beta = \alpha + (-\lambda) n$. ■

Πρόταση 2.8. Έστω $\alpha, n > 0$. Τότε ισχύει η ισοδυναμία: $x \equiv y \mod n \Leftrightarrow \alpha x \equiv \alpha y \mod \alpha n$
Απόδειξη: $x \equiv y \mod n \Leftrightarrow n \mid x - y \Leftrightarrow \alpha n \mid \alpha(x - y) = \alpha x - \alpha y \Leftrightarrow \alpha x \equiv \alpha y \mod \alpha n$. ■

Συνοψίζοντας τα παραπάνω έχουμε: **1ο:** Η σχέση $(\equiv \mod n)$, ως σχέση ισοδυναμίας, ορίζει μια **μοναδική διαμέριση** του $\mathbb{Z}$ σε **κλάσεις ισοδυναμίας**. Η κλάση ισοδυναμίας modulo n στην οποία ανήκει ο ακέραιος α θα συμβολίζεται με $\langle\alpha\rangle_n$ ή αν είναι δεδομένο το n, απλά με $\langle\alpha\rangle$. Η κλάση ισοδυναμίας στην οποία ανήκει το α αποτελείται από όλους τους ακεραίους που διαφέρουν από το α κατά ένα πολλαπλάσιο του n. Επομένως $\langle\boldsymbol{\alpha}\rangle_{\boldsymbol{n}} = \{\boldsymbol{\alpha + kn} \mid \boldsymbol{k} \in \mathbb{Z}\}$.
2ο: Σύμφωνα με την πρόταση 2.6, κάθε ακέραιος ανήκει στην ίδια κλάση ισοδυναμίας με το υπόλοιπο της διαίρεσής του με το n. Επειδή υπάρχουν ακριβώς n δυνατά υπόλοιπα, τα $0, 1, 2, \ldots, n-1$ και αυτά ανήκουν σε διαφορετικές κλάσεις ισοδυναμίας modulo n, υπάρχουν ακριβώς n κλάσεις ισοδυναμίας modulo n. Αυτές είναι οι: $\langle 0\rangle_n$, $\langle 1\rangle_n$, $\langle 2\rangle_n$,...,$\langle n-1\rangle_n$.

Ορισμός 2.9. Θα λέμε ότι οι ακέραιοι αριθμοί $\alpha_1, \alpha_2, \ldots, \alpha_n$ αποτελούν ένα **πλήρες σύστημα υπολοίπων modulo n** αν οι αντίστοιχες κλάσεις ισοδυναμίας $\langle\alpha_1\rangle_n$,$\langle\alpha_2\rangle_n$,..., $\langle\alpha_n\rangle_n$ είναι **όλες** οι κλάσεις ισοδυναμίας modulo n. Έτσι, οι αριθμοί $0, 1, 2, \ldots, n-1$ αποτελούν ένα πλήρες υπολοίπων modulo n. Το σύστημα αυτό είναι το μικρότερο σύστημα μη αρνητικών υπολοίπων.

Είναι σαφές ότι n ακέραιοι αποτελούν πλήρες υπολοίπων modulo n αν και μόνον αν είναι ανά δύο ανισοϋπόλοιποι modulo n.

Πρόταση 2.10. Αν n θετικός ακέραιος, τότε κάθε n διαδοχικοί ακέραιοι αποτελούν ένα πλήρες σύστημα υπολοίπων modulo n.
Απόδειξη: Έστω $k, k+1, k+2, \ldots, k+n-1$ διαδοχικοί ακέραιοι. Αν υποθέσουμε ότι $k+\lambda \equiv k+\mu \mod n$, όπου $0 \le \lambda < \mu \le n-1$, τότε $n \mid k+\mu-k-\lambda = \mu-\lambda > 0$. Επομένως $\mu-\lambda = tn$, όπου t θετικός ακέραιος. Άρα $\mu-\lambda = tn \ge n$. Αλλά $\mu-\lambda \le n-1 < n$, άτοπο. ■

Άσκηση 56. Δείξτε ότι οι αριθμοί $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ αποτελούν πλήρες σύστημα υπολοίπων modulo 11, ενώ οι αριθμοί $0, 1^2, 2^2, 3^2, \ldots, 10^2$ δεν αποτελούν τέτοιο σύστημα.
Απόδειξη: Για την πρώτη περίπτωση αρκεί να δείξουμε ότι οι αριθμοί $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ είναι ανά δύο ανισοϋπόλοιποι modulo 11. Προφανώς $2^k \not\equiv 0 \mod 11$, γιατί $(2^k, 11) = 1$, για κάθε $k = 0, 1, 2, \ldots, 9$. Αν $2^k \equiv 2^r \mod 11$, όπου $0 \le r < k \le 9$, τότε $11 \mid 2^k - 2^r = 2^r(2^{k-r}-1)$. Επειδή $(2^r, 11) = 1$, θα πρέπει $11 \mid 2^{k-r}-1 \Leftrightarrow 2^{k-r} \equiv 1 \mod 11$. Αλλά $0 < k-r \le 9$. Όμως $2^1 = 2 \mod 11$, $2^2 = 4 \mod 11$, $2^3 = 8 \mod 11$, $2^4 = 16 \equiv 5 \mod 11$, $2^5 \equiv 2\cdot 5 = 10 \mod 11$, $2^6 \equiv 20 \equiv 9 \mod 11$, $2^7 \equiv 18 \equiv 7 \mod 11$, $2^8 \equiv 14 \equiv 3 \mod 11$ και $2^9 \equiv 6 \mod 11$.
Για τη δεύτερη περίπτωση παρατηρούμε ότι $10^2 - 1^2 = (10-1)(10+1) = 9\cdot 11 \equiv 0 \mod 11$. Άρα οι αριθμοί 100 και 1 δεν είναι ανισοϋπόλοιποι modulo 11. $\big($Πιο απλά $100 - 1 = 99 \equiv 0 \mod 11\big)$. ■

Άσκηση 57. (i) Βρείτε ένα πλήρες σύστημα υπολοίπων modulo 11 που να αποτελείται **α)** από μόνον άρτιους ακεραίους και β) μόνον από περιττούς ακεραίους.
(ii) Είναι το σύνολο $\{-3, 34, 8, 12, -1, -11\}$ πλήρες σύστημα υπολοίπων modulo 6;
Λύση: (i) Ένα πλήρες σύστημα υπολοίπων modulo 11 είναι το $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. **α)** Προφανώς $(2, 11) = 1$. Άρα το $\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$ είναι πλήρες σύστημα υπολοίπων modulo 11, το οποίο αποτελείται μόνον από αρτίους. Μάλιστα $12 \equiv 1 \mod 11$, $14 \equiv 3 \mod 11$, $16 \equiv 5 \mod 11$, $18 \equiv 7 \mod 11$ και $20 \equiv 9 \mod 11$. **β)** Παρατηρούμε ότι $0 \equiv 11 \mod 11$, $2 \equiv 13 \mod 11$, $4 \equiv 15 \mod 11$, $6 \equiv 17 \mod 11$, $8 \equiv 19 \mod 11$ και $10 \equiv 21 \mod 11$. Άρα το $\{11, 1, 13, 3, 15, 5, 17, 7, 19, 9, 21\} = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21\}$ είναι πλήρες σύστημα υπολοίπων modulo 11, το οποίο αποτελείται μόνον από περιττούς. Ένα άλλο τέτοιο σύστημα είναι το $\{-11, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9\}$. $\big($Έχουμε $-11 \equiv 0 \mod 11, -9 \equiv 2 \mod 11, -7 \equiv 4 \mod 11, -5 \equiv 6 \mod 11, -3 \equiv 8 \mod 11$ και $-1 \equiv 10 \mod 11\big)$.
(ii) $-3 \equiv 3 \mod 6$, $34 \equiv 4 \mod 6$, $8 \equiv 2 \mod 6$, $12 \equiv 0 \mod 6$, $-1 \equiv 5 \mod 6$ και $-11 \equiv 1 \mod 6$. Όντως λοιπόν το σύνολο $\{-3, 34, 8, 12, -1, -11\}$ είναι ένα πλήρες σύστημα υπολοίπων modulo 6. ■

Άσκηση 58. Έστω $\alpha_1, \alpha_2, \ldots, \alpha_n$ n αριθμοί, όχι απαραίτητα διαφορετικοί. Δείξτε ότι υπάρχουν κάποιοι από αυτούς, των οποίων το άθροισμα διαιρείται με το n.

Απόδειξη: Θεωρούμε την ακολουθία των αριθμών $\alpha_1, \alpha_1+\alpha_2, \alpha_1+\alpha_2+\alpha_3, \ldots, \alpha_1+\alpha_2+\cdots+\alpha_n$. Αν οι n αυτοί αριθμοί ήταν ανισοϋπόλοιποι modulo n, τότε κάποιος από αυτούς θα ήταν ισοϋπόλοιπος modulo n με το μηδέν και άρα θα διαιρείτο από το n. Αν δεν ήσαν ανισοϋπόλοιποι modulo n, τότε θα υπήρχαν $\kappa, \lambda \in \{1, 2, \ldots, n\}$ με $\kappa < \lambda$ τέτοιοι, ώστε $\alpha_1+\alpha_2+\cdots+\alpha_\lambda \equiv \alpha_1+\alpha_2+\cdots+\alpha_\kappa \mod n \Leftrightarrow \alpha_{\kappa+1}+\cdots+\alpha_\lambda \equiv 0 \mod n$. ■

2.2 Η «περίεργη» αριθμητική modulo n και οι εφαρμογές της σε προβλήματα διαιρετότητας

Πρόταση 2.11. Ισχύουν τα ακόλουθα:
(i) Έστω $\alpha \equiv \beta \mod n$ και $\rho \in \mathbb{Z}$. Τότε $\rho\alpha \equiv \rho\beta \mod n$.
(ii) Έστω $\alpha_1 \equiv \beta_1 \mod n$ και $\alpha_2 \equiv \beta_2 \mod n$. Έστω επίσης $\kappa, \lambda \in \mathbb{Z}$. Τότε $\kappa\alpha_1+\lambda\alpha_2 \equiv \kappa\beta_1+\lambda\beta_2 \mod n$. Ιδιαιτέρως, αν $\alpha_1 \equiv \beta_1 \mod n$ και $\alpha_2 \equiv \beta_2 \mod n$, τότε $\alpha_1 \pm \alpha_2 \equiv \beta_1 \pm \beta_2 \mod n$.
(iii) Έστω $\alpha_1 \equiv \beta_1 \mod n$ και $\alpha_2 \equiv \beta_2 \mod n$. Τότε $\alpha_1\alpha_2 \equiv \beta_1\beta_2 \mod n$. Επαγωγικά, αν $\alpha_i \equiv \beta_i \mod n$, για κάθε $i = 1, 2, \ldots, k$, τότε $\alpha_1\alpha_2\cdots\alpha_k \equiv \beta_1\beta_2\cdots\beta_k \mod n$.
(iv) Έστω $\alpha \equiv \beta \mod n$ και k θετικός ακέραιος. Τότε $\alpha^k \equiv \beta^k \mod n$.
Απόδειξη: (i) Έστω $\alpha \equiv \beta \mod n \Leftrightarrow n \mid \alpha-\beta$. Επομένως $n \mid \rho(\alpha-\beta) = \rho\alpha-\rho\beta \Leftrightarrow \rho\alpha \equiv \rho\beta \mod n$.
(ii) $\alpha_1 \equiv \beta_1 \mod n \Leftrightarrow n \mid \alpha_1-\beta_1$ και $\alpha_2 \equiv \beta_2 \mod n \Leftrightarrow n \mid \alpha_2-\beta_2$.
Επομένως $n \mid \kappa(\alpha_1-\beta_1)+\lambda(\alpha_2-\beta_2) = (\kappa\alpha_1+\lambda\alpha_2)-(\kappa\beta_1+\lambda\beta_2) \Leftrightarrow \kappa\alpha_1+\lambda\alpha_2 \equiv \kappa\beta_1+\lambda\beta_2 \mod n$.
(iii) Έχουμε $n \mid \alpha_1-\beta_1$ και $n \mid \alpha_2-\beta_2$. Επομένως $\alpha_1\alpha_2-\beta_1\beta_2 = \alpha_1\alpha_2-\alpha_1\beta_2+\alpha_1\beta_2-\beta_1\beta_2 = \alpha_1(\alpha_2-\beta_2)+\beta_2(\alpha_1-\beta_1)$ που είναι πολλαπλάσιο του n. Άρα $\alpha_1\alpha_2 \equiv \beta_1\beta_2 \mod n$. Υποθέτουμε τώρα ότι αν $k \geq 2$ και $\alpha_i \equiv \beta_i \mod n$, για κάθε $i = 1, 2, \ldots, k$, τότε $\alpha_1\alpha_2\cdots\alpha_k \equiv \beta_1\beta_2\cdots\beta_k \mod n$. Τότε, αν $\alpha_{k+1} \equiv \beta_{k+1} \mod n$, (εφόσον το αποτέλεσμα ισχύει για δύο σχέσεις), $\alpha_1\alpha_2\cdots\alpha_k\alpha_{k+1} \equiv \beta_1\beta_2\cdots\beta_k\beta_{k+1} \mod n$.
(iv) Προκύπτει από το προηγούμενο αν θέσουμε $\alpha_1 = \alpha_2 = \cdots = \alpha_k = \alpha$ και $\beta_1 = \beta_2 = \cdots = \beta_k = \beta$. ■

Άσκηση 59. Να δείξετε ότι $7 \mid 2222^{5555}+5555^{2222}$.
Απόδειξη: Ο αριθμός $2222^{5555}+5555^{2222}$ είναι τρομακτικά μεγάλος. Στην αρχή θα προσπαθήσουμε να «ροκανίσουμε» τις βάσεις. Εφόσον κάθε αριθμός είναι ισοδύναμος modulo 7 με το υπόλοιπο της διαίρεσής του με το 7, έχουμε: $2222 = 317 \cdot 7 + 3 \Rightarrow 2222 \equiv 3 \mod 7$. Από το (iv) της προηγούμενης πρότασης προκύπτει ότι $2222^{5555} \equiv 3^{5555} \mod 7$. Παρατηρούμε ότι $3^2 = 9 \equiv 2 \mod 7$. Άρα $3^3 \equiv 3 \cdot 2 = 6 \equiv -1 \mod 7$, σύμφωνα με το (i) της προηγούμενης πρότασης. Συνεπώς $3^6 = (3^3)^2 \equiv (-1)^2 = 1 \mod 7$. Οι 6^{η} δύναμη του 3 είναι λοιπόν ισοϋπόλοιπη modulo 7 με το 1. Άρα και οι δυνάμεις της $6^{\eta\varsigma}$ δύναμης του 3 θα είναι ισοϋπόλοιπες modulo 7 με το 1. Πόσες φορές χωράει το 6 στο 5555; Δεν έχουμε παρά να διαιρέσουμε το 5555 δια του 6. Έχουμε $5555 = 6 \cdot 925 + 5$. Επομένως $3^{5555} = 3^{6\cdot 925+5} = (3^6)^{925} \cdot 3^5 \equiv 1^{925} \cdot 3^5 = 3^5 = 3^3 \cdot 3^2 = 27 \cdot 9 \equiv 6 \cdot 2 = 12 \equiv 5 \mod 7$. Με άλλα λόγια, το 5 είναι το υπόλοιπο της διαίρεσης του 3^{5555} άρα και του 2222^{5555} δια του 7. Όχι και τόσο άσχημα.
Επαναλαμβάνουμε τώρα την προηγούμενη διαδικασία στο 5555^{2222}. Έχουμε: $5555 = 7\cdot 793+4 \Leftrightarrow 5555 \equiv 4 \mod 7 \Rightarrow 5555^{2222} \equiv 4^{2222} \mod 7$. Επίσης $4^2 = 16 \equiv 2 \mod 7$, $4^3 \equiv 4\cdot 2 = 8 \equiv 1 \mod 7$. Τώρα διαιρούμε το 2222 δια του 3 και παίρνουμε $2222 = 3 \cdot 740 + 2$. Επομένως $5555^{2222} \equiv 4^{2222} = 4^{3\cdot 740+2} = (4^3)^{740} \cdot 4^2 \equiv \equiv 1 \cdot 16 \equiv 2 \mod 7$. Τελικώς $2222^{5555}+5555^{2222} \equiv 5+2 = 7 \equiv 0 \mod 7 \Leftrightarrow 7 \mid 2222^{5555}+5555^{2222}$. ■

Άσκηση 60. Να δείξετε ότι $39 \mid 7^{37}+13^{37}+19^{37}$.
Απόδειξη: $39 = 3 \cdot 13$ και $(3, 13) = 1$. Αρκεί να δείξουμε ότι το 3 και το 13 διαιρούν την δοσμένη παράσταση. Έχουμε: $7 \equiv 1 \mod 3 \Rightarrow 7^{37} \equiv 1^{37} = 1 \mod 3$, $13 \equiv 1 \mod 3 \Rightarrow 13^{37} \equiv 1 \mod 3$ και $19 \equiv 1 \mod 3 \Rightarrow 19^{37} \equiv 1 \mod 3$. Συνεπώς $7^{37}+13^{37}+19^{37} \equiv 1+1+1 = 3 \equiv 0 \mod 3$. Ακόμη $7^2 = 49 \equiv 10 \mod 13$, $7^3 \equiv 70 \equiv 5 \mod 13$, $7^4 \equiv 35 \equiv 9 \mod 13$, $7^5 \equiv 63 \equiv 11 \mod 13$, $7^6 \equiv 77 \equiv 12 \equiv -1 \mod 13$. Άρα $7^{12} \equiv 1 \mod 13 \Rightarrow 7^{37} = (7^{12})^3 \cdot 7 \equiv 1 \cdot 7 = 7 \mod 13$. Ακόμη, $13^{37} \equiv 0 \mod 13$, γιατί $13 \equiv 0 \mod 13$ και $19 \equiv 6 \mod 13 \Rightarrow 19^2 \equiv 36 \equiv -3 \mod 13 \Rightarrow 19^4 \equiv (-3)^2 = 9 \equiv -4 \mod 13 \Rightarrow 19^{12} \equiv (-4)^3 = -64 \equiv -12 \equiv 1 \mod 13$. Άρα $19^{37} = (19^{12})^3 \cdot 19 \equiv 19 \equiv 6 \mod 13$. Τελικώς $7^{37}+13^{37}+19^{37} \equiv 7+0+6 = 13 \equiv 0 \mod 13$. ■

Άσκηση 61. Δείξτε ότι, για κάθε θετικό ακέραιο n, ο αριθμός $49^n - 2352n - 1$ διαιρείται με το 2304.
Απόδειξη: Παρατηρούμε ότι $2304 = 2^8 \cdot 3^2$. Θα αποδείξουμε ότι $49^n - 2352n - 1 \equiv 0 \mod 8$ και $49^n - 2352n - 1 \equiv 0 \mod 9$. Για $n = 1$ έχουμε $49^n - 2352n - 1 = 49 - 2352 - 1 = -2304 \equiv 0 \mod 2304$. Υποθέτουμε ότι $49^n - 2352n - 1 \equiv 0 \mod 8$. Τότε $49^{n+1} - 2352(n+1) - 1 = 49 \cdot 49^n - 2352n - 2352 - 1 \equiv$ $\equiv 1 \cdot 49^n - 2352n - 8 \cdot 294 - 1 = 49^n - 2352n - 0 - 1 = 49^n - 2352n - 1 \equiv 0 \mod 8$.
Υποθέτουμε τώρα ότι $49^n - 2352n - 1 \equiv 0 \mod 9$. Τότε $49^{n+1} - 2352(n+1) - 1 = 49 \cdot 49^n - 2352n -$ $-2352 - 1 \equiv 4 \cdot 49^n - 4 \cdot 2352n - 4 + 3 \cdot 2352n - 2352 + 3 = 4 \cdot (49^n - 2352n - 1) + 3 \cdot 2352n - 2349 \equiv$ $\equiv 0 + 9 \cdot 784n - 9 \cdot 261 \equiv 0 \mod 9$. ■

Άσκηση 62. Έστω $\alpha+\beta \neq 0$ και n περιττός θετικός ακέραιος. Τότε $\left(\dfrac{\alpha^n+\beta^n}{\alpha+\beta}, \alpha+\beta\right) = (n(\alpha,\beta)^{n-1}, \alpha+\beta)$.
Απόδειξη: Υποθέτουμε αρχικά ότι $\alpha + \beta > 0$. Θέτουμε $h = \alpha + \beta$. Τότε $\alpha = h - \beta \equiv -\beta \mod h \Rightarrow$ $\alpha^k \equiv (-1)^k \beta^k \mod h$, για κάθε μη αρνητικό ακέραιο k. Επομένως $\dfrac{\alpha^n+\beta^n}{\alpha+\beta} = \displaystyle\sum_{k=0}^{n-1} (-1)^k \alpha^{n-1-k}\beta^k \equiv$

$(-1)^{n-1} n\beta^{n-1} \underset{n-1 \text{ άρτιος}}{=} n\beta^{n-1} \mod h$, δηλαδή $\dfrac{\alpha^n+\beta^n}{\alpha+\beta} = n\beta^{n-1} + \lambda \cdot h$, για κάποιο $\lambda \in \mathbb{Z}$.
Επομένως $\left(\dfrac{\alpha^n+\beta^n}{\alpha+\beta}, \alpha+\beta\right) = (n\beta^{n-1} + \lambda \cdot h, h) = (n\beta^{n-1}, h)$.
Ομοίως $\beta = h - \alpha \equiv -\alpha \mod h \Rightarrow \beta^k \equiv (-1)^k \alpha^k \mod h$, για κάθε μη αρνητικό ακέραιο k. Επομένως $\dfrac{\alpha^n+\beta^n}{\alpha+\beta} = \displaystyle\sum_{k=0}^{n-1} (-1)^k \alpha^{n-1-k}\beta^k \equiv n\alpha^{n-1} \mod h$ και, όπως παραπάνω $\left(\dfrac{\alpha^n+\beta^n}{\alpha+\beta}, \alpha+\beta\right) = (n\alpha^{n-1}, h)$.
Τελικώς $\delta := \left(\dfrac{\alpha^n+\beta^n}{\alpha+\beta}, \alpha+\beta\right) = (n\alpha^{n-1}, h) = (n\beta^{n-1}, h)$.
Συνεπώς $\delta = (\delta, \delta) = ((n\alpha^{n-1}, h), (n\beta^{n-1}, h)) = (n\alpha^{n-1}, n\beta^{n-1}, h) = (n(\alpha^{n-1}, \beta^{n-1}), h) = (n(\alpha,\beta)^{n-1}, h) =$ $= (n(\alpha,\beta)^{n-1}, \alpha+\beta)$.
Αν τώρα $\alpha + \beta < 0$, έχουμε $\left(\dfrac{\alpha^n+\beta^n}{\alpha+\beta}, \alpha+\beta\right) = \left(\dfrac{(-\alpha)^n+(-\beta)^n}{-\alpha-\beta}, -\alpha-\beta\right) = (n(-\alpha,-\beta)^{n-1}, -\alpha-\beta) =$ $= (n(\alpha,\beta)^{n-1}, \alpha+\beta)$. ■

Άσκηση 63. **(i)** Βρείτε το υπόλοιπο της διαίρεσης $\dfrac{36!}{26!} : 13$.
(ii) Δείξτε ότι $12 \mid 169^{323} + 323^{169}$.
(iii) Εξετάστε αν **α)** $227 \mid 3^{32} + 8$ και **β)** $117 \mid 5^{53} - 1$.
Λύση: **(i)** $\dfrac{36!}{26!} = 27 \cdot 28 \cdot 29 \cdot 30 \cdot 31 \cdot 32 \cdot 33 \cdot 34 \cdot 35 \cdot 36 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv 24 \cdot 30 \cdot 56 \cdot 90 \equiv 11 \cdot 4 \cdot 4 \cdot 12 \equiv$ $\equiv (-2) \cdot 16 \cdot (-1) \equiv 2 \cdot 3 = 6 \mod 13$. Το υπόλοιπο της διαίρεσης $\dfrac{36!}{26!} : 13$ είναι λοιπόν 6.
(ii) Έχουμε $169 = 14 \cdot 12 + 1 \Rightarrow 169 \equiv 1 \mod 12 \Rightarrow 169^{323} \equiv 1 \mod 12$. Επίσης $323 = 26 \cdot 12 + 11 \Rightarrow$ $323 \equiv 11 \equiv -1 \mod 12 \Rightarrow 323^{169} \equiv (-1)^{169} = -1 \mod 12$. Επομένως $169^{323} + 323^{169} \equiv 1 - 1 = 0 \mod 12$.
(iii) α) $3^4 = 81$. Άρα $3^8 = 81^2 = 6561 = 28 \cdot 227 + 205 \equiv 205 \equiv -22 \mod 227$. Επομένως $3^{32} = (3^8)^4 \equiv$ $\equiv (-22)^4 = 22^2 \cdot 22^2 = 484 \cdot 484 \equiv 30^2 = 900 = 3 \cdot 227 + 219 \equiv 219 \equiv -8 \mod 227$. Άρα $3^{32} + 8 \equiv -8 + 8 = 0 \mod 227 \Leftrightarrow 227 \mid 3^{32} + 8$.
β) $117 = 9 \cdot 13$. Έχουμε $5^2 = 25 \equiv 7 \mod 9 \Rightarrow 5^3 \equiv 5 \cdot 7 = 35 \equiv 8 \equiv -1 \mod 9$. Επίσης $53 = 3 \cdot 17 + 2$. Επομένως $5^{53} = (5^3)^{17} \cdot 5^2 \equiv (-1)^{17} \cdot 7 = -7 \mod 9 \Rightarrow 5^{53} - 1 \equiv -8 \equiv 1 \mod 9 \Rightarrow 9 \nmid 5^{53} - 1$. Άρα και $117 \nmid 5^{53} - 1$. ■

Άσκηση 64. **(i)** Βρείτε το υπόλοιπο της διαίρεσης $1! + 2! + 3! + 4! + \cdots + 99! + 100! : 12$.
(ii) Δείξτε ότι $41 \mid 2^{20} - 1$.
Λύση: **(i)** Παρατηρούμε ότι $12 \mid 4! = 24$ και επομένως $12 \mid k!$, για κάθε $k \geq 4$. Άρα $1! + 2! + 3! + 4! + \cdots +$ $+99! + 100! \equiv 1 + 2 + 6 = 9 \mod 12$. Άρα το υπόλοιπο της διαίρεσης είναι 9.
(ii) $2^5 = 32 \equiv -9 \mod 41$. Άρα $2^{10} \equiv (-9)^2 = 81 = 82 - 1 \equiv -1 \mod 41$. Επομένως $2^{20} \equiv 1 \mod 41 \Leftrightarrow 2^{20} - 1 \equiv 0 \mod 41$. ■

Άσκηση 65. (i) Βρείτε τα υπόλοιπα των διαιρέσεων των αριθμών 2^{50} και 41^{65} με το 7.
(ii) Ποιο είναι το υπόλοιπο της διαίρεσης $1^5+2^5+3^5+4^5+\cdots+99^5+100^5 : 4$;
(iii) Δείξτε ότι $39 \mid 53^{103}+103^{53}$ και $7 \mid 111^{333}+333^{111}$.
Λύση: (i) $2^3 = 8 \equiv 1 \mod 7 \Rightarrow 2^{48} = (2^3)^{16} \equiv 1 \mod 7$. Άρα $2^{50} \equiv 4 \mod 7$. $41 = 5\cdot 7+6 \equiv 6 \equiv -1 \mod 7$. Επομένως $41^{65} \equiv (-1)^{65} = -1 \equiv 6 \mod 7$.
(ii) Αν $n = 2\rho \in \{1,2,\ldots,100\}$, τότε $n^5 = 32\rho^5 \equiv 0 \mod 4$. Αν $n = 2\rho+1 \in \{1,2,\ldots,100\}$, τότε $n^5 = (2\rho+1)^5 = ((2\rho+1)^2)^2\cdot(2\rho+1) = (4\rho^2+4\rho+1)^2\cdot(2\rho+1) \equiv 1\cdot(2\rho+1) = 2\rho+1 \mod 4$, για κάθε $\rho = 0,1,2,\ldots,49$. Αν λοιπόν $\rho = 2\sigma$ άρτιος, τότε $n^5 \equiv 4\sigma+1 \equiv 1 \mod 4$, ενώ αν $\rho = 2\sigma+1$ περιττός, τότε $n^5 \equiv 4\sigma+3 \equiv 3 \mod 4$. Στο σύνολο $0,1,2,\ldots,49$ υπάρχουν 25 άρτιοι και 25 περιττοί. Επομένως $1^5+2^5+3^5+\cdots+99^5+100^5 \equiv 25\cdot 1+25\cdot 3 = 100 \equiv 0 \mod 4$.
(iii) Έχουμε $39 = 3\cdot 13$. Τώρα $53 = 17\cdot 3+2 \equiv 2 \mod 3$. Επομένως $53^2 \equiv 4 \equiv 1 \mod 3 \Rightarrow (53)^{103} = (53^2)^{51}\cdot 53 \equiv 1\cdot 2 = 2 \mod 3$. Επίσης $103 = 3\cdot 34+1 \equiv 1 \mod 3$. Επομένως $103^{53} \equiv 1 \mod 3$. Συμπεραίνουμε ότι $53^{103}+103^{53} \equiv 2+1 = 3 \equiv 0 \mod 3 \Leftrightarrow 3 \mid 53^{103}+103^{53}$.
Ακόμη, $53 = 4\cdot 13+1 \equiv 1 \mod 13 \Rightarrow 53^{103} \equiv 1 \mod 13$. Επίσης, $103 = 7\cdot 13+12 \equiv 12 \equiv -1 \mod 13 \Rightarrow 103^{53} \equiv (-1)^{53} = -1 \mod 13$. Συμπεραίνουμε ότι $53^{103}+103^{53} \equiv 1-1 = 0 \mod 13 \Leftrightarrow \Leftrightarrow 13 \mid 53^{103}+103^{53}$.
$111 = 15\cdot 7+6 \equiv 6 \equiv -1 \mod 7$. Άρα $111^{333} \equiv (-1)^{333} = -1 \mod 7$. Ομοίως $333 = 47\cdot 7+4 \equiv 4 \mod 7$. Ακόμη $333^2 \equiv 4^2 = 16 \equiv 2 \mod 7$ και $333^3 \equiv 2\cdot 4 = 8 \equiv 1 \mod 7 \Rightarrow 333^{111} = (333^3)^{37} \equiv 1 \mod 7$. Άρα $111^{333}+333^{111} \equiv -1+1 = 0 \mod 7$. ■

Άσκηση 66. Δείξτε ότι: **(i)** $13 \mid 3^{n+2}+4^{2n+1}$ και **(ii)** $43 \mid 6^{n+2}+7^{2n+1}$, για κάθε θετικό ακέραιο n.
Λύση: (i) $3^{n+2}+4^{2n+1} = 9\cdot 3^n+4\cdot(4^2)^n = 9\cdot 3^n+4\cdot 16^n \underset{16\equiv 3 \mod 13}{\equiv} 9\cdot 3^n+4\cdot 3^n = 13\cdot 3^n \equiv 0 \mod 13$.
(ii) $6^{n+2}+7^{2n+1} = 36\cdot 6^n+7\cdot(7^2)^n = 36\cdot 6^n+7\cdot(49)^n \underset{49\equiv 6 \mod 43}{\equiv} 36\cdot 6^n+7\cdot 6^n = 43\cdot 3^n \equiv 0 \mod 43$. ■

Πρόταση 2.12. (*b*-αδική παράσταση αριθμού) Έστω $b \in \mathbb{Z}$ με $b \geq 2$. Τότε για κάθε θετικό ακέραιο α υπάρχει μοναδικός φυσικός αριθμός n και $\kappa_0, a_1, \ldots, \kappa_n$, με $0 \leq \kappa_i \leq b-1$, για κάθε $i = 0,\ldots,n$ τέτοιοι, ώστε

$$\alpha = \kappa_n b^n + \kappa_{n-1}b^{n-1} + \cdots + \kappa_1 b + \kappa_0,$$

με $\kappa_n \neq 0$.
Απόδειξη: Ύπαρξη: Εφαρμόζουμε επαγωγή επί του α. Αν $\alpha = 1$ (ή γενικότερα αν $\alpha < b$), τότε θέτουμε $\kappa_0 = \alpha$ και $n = 0$ και τελειώσαμε. Έστω τώρα ότι $\alpha > 1$ και υποθέτουμε ότι κάθε θετικός ακέραιος μικρότερος του α γράφεται στην παραπάνω μορφή. Διαιρούμε το α με το b και παίρνουμε $\alpha = b\pi+\upsilon$, όπου $0 \leq \upsilon < b$. Παρατηρούμε ότι $\pi \geq 0$. Πράγματι, αν $\pi \leq -1$, τότε $\alpha = b\pi+\upsilon \leq -b+\upsilon < 0$, άτοπο. $\big($Αυτό δεν χρειαζόταν γιατί ξέρουμε ότι $\pi = \left\lfloor \frac{\alpha}{b} \right\rfloor \geq 0\big)$. Θέτουμε $\kappa_0 = \upsilon$. Αν $\pi = 0$, τότε $\alpha = \kappa_0 b^0$ και τελειώσαμε. Αν $\pi > 0$, τότε παρατηρούμε ότι $0 < \pi = \frac{\alpha-\upsilon}{b} \leq \frac{\alpha}{b} < \alpha$, γιατί $b > 1$. Από την επαγωγική υπόθεση προκύπτει ότι το π γράφεται στη μορφή $\pi = \kappa_n b^{n-1}+\kappa_{n-1}b^{n-2}+\cdots+\kappa_2 b+\kappa_1$, για κάποιο $n \geq 1$, με $0 \leq \kappa_i < b$, για κάθε $i = 1,\ldots,n$ και $\kappa_n \neq 0$. Επομένως, $\alpha = b(\kappa_n b^{n-1}+\kappa_{n-1}b^{n-2}+\cdots+\kappa_1)+\kappa_0 = \kappa_n b^n+\kappa_{n-1}b^{n-1}+\cdots+\kappa_1 b+\kappa_0$.
Μοναδικότητα: Έστω $\alpha = \kappa_n b^n+\kappa_{n-1}b^{n-1}+\cdots+\kappa_1 b+\kappa_0$ όπως παραπάνω. Υποθέτουμε ότι $\alpha = \lambda_m b^m+\lambda_{m-1}b^{m-1}+\cdots+\lambda_1 b+\lambda_0$, για κάποιο $m \geq 0$, με $0 \leq \lambda_i < b$, για κάθε $i = 0,1,\ldots,m$ και $\lambda_m \neq 0$. Αρχικώς θα αποδείξουμε ότι $m = n$. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $n > m$. Τότε έχουμε: $\alpha = \lambda_m b^m+\lambda_{m-1}b^{m-1}+\cdots+\lambda_1 b+\lambda_0 \leq (b-1)b^m+(b-1)b^{m-1}+\cdots+(b-1)b+(b-1) = (b-1)(b^m+b^{m-1}+\cdots+b+1) = (b-1)\frac{b^{m+1}-1}{b-1} = b^{m+1}-1 < b^{m+1} \leq b^n \leq \kappa_n b^n+\kappa_{n-1}b^{n-1}+\cdots+\kappa_1 b+\kappa_0 = \alpha$, άτοπο. Άρα $m = n$.
Τώρα, με επαγωγή επί του $n = m$ θα αποδείξουμε ότι από τη σχέση $\kappa_n b^n+\kappa_{n-1}b^{n-1}+\cdots+\kappa_1 b+\kappa_0 = \lambda_n b^n+\lambda_{n-1}b^{n-1}+\cdots+\lambda_1 b+\lambda_0$ προκύπτει ότι $\kappa_i = \lambda_i$, για κάθε $i = 0,1,2,\ldots,n$. Για $n = 0$ έχουμε $\lambda_0 = \kappa_0$, δηλαδή αυτό που θέλουμε.
Έστω τώρα ότι $n > 0$. Παρατηρούμε ότι $\alpha = b(\kappa_n b^{n-1}+\cdots+\kappa_1)+\kappa_0 = b(\lambda_n b^{n-1}+\cdots+\lambda_1)+\lambda_0$, με $0 \leq \leq \kappa_0, \lambda_0 < b$. Επομένως οι αριθμοί κ_0, λ_0 είναι ίσα με ίσα με το υπόλοιπο της διαίρεσης $\alpha : b$ και οι αριθμοί $\kappa_n b^{n-1}+\cdots+\kappa_1$ και $\lambda_n b^{n-1}+\cdots+\lambda_1$ είναι ίσοι με το πηλίκο της διαίρεσης $\alpha : b$. Άρα $\kappa_0 = \lambda_0$

και $\kappa_n b^{n-1} + \cdots + \kappa_1 = \lambda_n b^{n-1} + \cdots + \lambda_1$. Η μεγαλύτερη δύναμη του b στα τελευταία αθροίσματα είναι $n-1 < n$ και επομένως από την επαγωγική υπόθεση $\kappa_1 = \lambda_1, \kappa_2 = \lambda_2, \ldots, \kappa_n = \lambda_n$, . ■

Παρατηρούμε ότι το μηδέν δεν γράφεται στη μορφή $0 = \kappa_n b^n + \kappa_{n-1} b^{n-1} + \cdots + \kappa_1 b + \kappa_0$ με $n \geq 0$, $0 \leq \kappa_i < b$, για κάθε $i = 0, 1, \ldots, n$ και $\kappa_n > 0$. (Διότι $0 < \kappa_n \leq \kappa_n b^n \leq \kappa_n b^n + \kappa_{n-1} b^{n-1} + \cdots + \kappa_1 b + \kappa_0$). Δεχόμαστε λοιπόν ότι το μηδέν θα γράφεται απλώς $\kappa_0 b^0 = 0 \cdot b^0$, δηλαδή $\kappa_0 = 0$. Καταλήγουμε λοιπόν στο επόμενο πόρισμα:

Πόρισμα 2.13. Έστω α φυσικός αριθμός (μη αρνητικός ακέραιος). Τότε το α γράφεται μονοσημάντως στη μορφή

$$\alpha = \kappa_n b^n + \kappa_{n-1} b^{n-1} + \cdots + \kappa_1 b + \kappa_0,$$

όπου $n \geq 0$ και $0 \leq \kappa_i < b$, για κάθε $i = 0, 1, \ldots, n$, υπό τις εξής προϋποθέσεις:
α) $\kappa_n \neq 0 \Leftrightarrow \alpha > 0$ και
β) $n = 0$ και $\kappa_0 = 0$, αν και μόνον αν $\alpha = 0$.
Η ανωτέρω παράσταση ονομάζεται ***b*-αδική παράσταση του αριθμού α** και οι αριθμοί $\kappa_0, \kappa_1, \ldots, \kappa_n$ **ψηφία του α με βάση το b**. ■

Συμβολισμός: Αν $\alpha = \kappa_n b^n + \kappa_{n-1} b^{n-1} + \cdots + \kappa_1 b + \kappa_0$, όπως προηγουμένως, τότε γράφουμε

$$\boldsymbol{\alpha = (\kappa_n \kappa_{n-1} \cdots \kappa_1 \kappa_0)_b}$$

για να παραστήσουμε την b-αδική παράσταση του α. Υπενθυμίζουμε ότι τα συνηθέστερα συστήματα αρίθμησης είναι το δεκαδικό ($b = 10$) και το δυαδικό ($b = 2$). Το τελευταίο έχει ιδιαίτερη εφαρμογή στην πληροφορική.

Πόρισμα 2.14. Έστω $\alpha = (\kappa_n \kappa_{n-1} \cdots \kappa_1 \kappa_0)_{10} = \kappa_n 10^n + \kappa_{n-1} 10^{n-1} + \cdots + \kappa_1 10 + \kappa_0$ θετικός ακέραιος. Τότε:
(i) $2 \mid \alpha \Leftrightarrow \kappa_0 = 0$ ή 2 ή 4 ή 6 ή 8.
(ii) $5 \mid \alpha \Leftrightarrow \kappa_0 = 0$ ή 5.
Απόδειξη: Άμεση, γιατί $\alpha \equiv \kappa_0 \mod 10$, οπότε $\alpha \equiv \kappa_0 \mod 2$ και $\alpha \equiv 0 \mod 5$. Άρα ο α διαιρείται με το 2 αν και μόνον αν ο κ_0 είναι άρτιος, δηλαδή 0, 2, 4, 6 ή 8. Επίσης ο α διαιρείται με το 5 αν και μόνον αν ο κ_0 διαιρείται με το 5, δηλαδή είναι 0 ή 5. ■

Η επόμενη πρόταση δίδει μια απόδειξη των γνωστών εμπειρικών κανόνων διαιρετότητας στο δεκαδικό σύστημα, αλλά και άλλων κανόνων.

Πρόταση 2.15. (Κριτήρια διαιρετότητας) Έστω $\alpha = (\kappa_n \kappa_{n-1} \cdots \kappa_1 \kappa_0)_{10}$ θετικός ακέραιος.
(i) Ο α διαιρείται με το 9 αν και μόνον αν το άθροισμα $\kappa_n + \kappa_{n-1} + \cdots + \kappa_1 + \kappa_0$ των ψηφίων του διαιρείται με το 9.
(ii) Ο α διαιρείται με το 3 αν και μόνον αν το άθροισμα $\kappa_n + \kappa_{n-1} + \cdots + \kappa_1 + \kappa_0$ των ψηφίων του διαιρείται με το 3.
(iii) Ο α διαιρείται με το 11 αν και μόνον αν ο αριθμός $\kappa_0 - \kappa_1 + \kappa_2 - \cdots + (-1)^n \kappa_n$ διαιρείται με το 11.
Απόδειξη: (i), **(ii)** Παρατηρούμε ότι $10 \equiv 1 \mod 9$, άρα $10^k \equiv 1 \mod 9$, για κάθε μη αρνητικό ακέραιο k. Επομένως $\alpha = \kappa_n 10^n + \kappa_{n-1} 10^{n-1} + \cdots + \kappa_1 10 + \kappa_0 \equiv \kappa_n + \kappa_{n-1} + \cdots + \kappa_1 + \kappa_0 \mod 9$.
(iii) Παρατηρούμε ότι $10 \equiv -1 \mod 11$, άρα $10^k \equiv (-1)^k \mod 11$, για κάθε μη αρνητικό ακέραιο k. Επομένως $\alpha = \kappa_n 10^n + \kappa_{n-1} 10^{n-1} + \cdots + \kappa_1 10 + \kappa_0 \equiv \kappa_n (-1)^n + \kappa_{n-1} (-1)^{n-1} + \cdots - \kappa_1 + \kappa_0 \mod 11$. ■

Άσκηση 67. (i) Αν $n \geq 3$, τότε ο α διαιρείται με το 7, το 11 ή το 13 αν και μόνον αν ο αριθμός $(\kappa_n \kappa_{n-1} \cdots \kappa_3)_{10} - (\kappa_2 \kappa_1 \kappa_0)_{10}$ έχει την ίδια ιδιότητα.
(ii) Αν $n \geq 3$, τότε ο α διαιρείται με το 27 ή το 37 αν και μόνον αν ο αριθμός $(\kappa_n \kappa_{n-1} \cdots \kappa_3)_{10} + (\kappa_2 \kappa_1 \kappa_0)_{10}$ έχει την ίδια ιδιότητα.
Απόδειξη: (i) $\alpha - 10^3 \cdot ((\kappa_n \kappa_{n-1} \cdots \kappa_3)_{10} - (\kappa_2 \kappa_1 \kappa_0)_{10}) = (10^3 + 1)(\kappa_2 \cdot 10^2 + \kappa_1 \cdot 10 + \kappa_0) = 1001(\kappa_2 \cdot 10^2 + \kappa_1 \cdot 10 + \kappa_0) \equiv 0 \mod 7, 11, 13$, γιατί $7 \mid 1001$, $11 \mid 1001$ και $13 \mid 1001$. Αν κάποιος από τους 7, 11 και 13 διαιρεί τον α, τότε θα διαιρεί και τον $10^3 \cdot ((\kappa_n \kappa_{n-1} \cdots \kappa_3)_{10} - (\kappa_2 \kappa_1 \kappa_0)_{10})$ και αντιστρόφως. Επειδή

$(10^3,7)=(10^3,11)=(10^3,13)=1$, αυτό συμβαίνει όταν και μόνον όταν κάποιος από τους 7, 11 και 13 διαιρεί τον $(\kappa_n\kappa_{n-1}\cdots\kappa_3)_{10}-(\kappa_2\kappa_1\kappa_0)_{10}$.
(ii) $\alpha-10^3\cdot((\kappa_n\kappa_{n-1}\cdots\kappa_3)_{10}+(\kappa_2\kappa_1\kappa_0)_{10})=-(10^3-1)(\kappa_2\cdot10^2+\kappa_1\cdot10+\kappa_0)=-999\cdot(\kappa_2\cdot10^2+\kappa_1\cdot10+\kappa_0)\equiv0 \mod 27,37$, γιατί $27\mid999$ και $37\mid999$. Αν λοιπόν κάποιος από τους 27 και 37 διαιρεί τον α, τότε θα διαιρεί και τον $10^3\cdot((\kappa_n\kappa_{n-1}\cdots\kappa_3)_{10}+(\kappa_2\kappa_1\kappa_0)_{10})$ και αντιστρόφως. Επειδή $(10^3,27)=(10^3,37)=1$, αυτό συμβαίνει όταν και μόνον όταν κάποιος από τους 27 και 37 διαιρεί τον $(\kappa_n\kappa_{n-1}\cdots\kappa_3)_{10}+(\kappa_2\kappa_1\kappa_0)_{10}$. ■

Άσκηση 68. (i) Βρείτε τα τρία τελευταία ψηφία (στο δεκαδικό σύστημα) του $2^{100}-1$.
(ii) Βρείτε τα δύο τελευταία ψηφία (στο δεκαδικό σύστημα) του αριθμού 9^{99}.
Λύση: (i) $2^{10}=1024\equiv24 \mod 1000\Rightarrow2^{20}\equiv24^2=576 \mod 1000\Rightarrow2^{30}\equiv576\cdot24=13824\equiv824 \mod 1000$. Άρα $2^{50}=2^{30}\cdot2^{20}\equiv824\cdot576=474624\equiv624 \mod 1000$. Επομένως $2^{100}=(2^{50})^2\equiv624^2=$ $=389376\equiv376 \mod 1000$. Άρα $2^{100}-1\equiv375 \mod 1000$, δηλαδή ο αριθμός $2^{100}-1$ λήγει σε 375.
(ii) $9^3=729\equiv29 \mod 100\Rightarrow9^6\equiv29^2=841\equiv41 \mod 100\Rightarrow9^{12}\equiv41^2=1681\equiv81=9^2 \mod 100$. Επομένως $9^{12}-9^2\equiv0 \mod 100\Leftrightarrow9^2(9^{10}-1)\equiv0 \mod 100$ και επειδή $(9^2,100)=1$, $9^{10}\equiv1 \mod 100$. Επομένως $9^{99}\cdot9=9^{100}\equiv1 \mod 100$. Επίσης $9(-11)=-99\equiv1 \mod 100$. Επομένως $9(9^{99}-(-11))\equiv0 \mod 100 \underset{(9,100)=1}{\Leftrightarrow} 9^{99}\equiv-11\equiv89 \mod 100$. Άρα ο αριθμός 9^{99} λήγει σε 89. ■

Σημειώνουμε εδώ ότι η παραπάνω άσκηση μπορεί να λυθεί ευκολότερα με τη χρήση της συνάρτησης φ του Euler. Γενικά, αν θέλουμε να υπολογίσουμε το υπόλοιπο της διαίρεσης μιας μεγάλης δύναμης με έναν αριθμό, υψώνουμε συνεχώς στο τετράγωνο, δηλαδή εκφράζουμε τον εκθέτη στη δυαδική μορφή. Ας δούμε την επόμενη άσκηση:

Άσκηση 69. Να βρείτε τα τρία τελευταία ψηφία του αριθμού 11^{1492}.
Λύση: Έχουμε $11=11 \mod 1000$, $11^2=121 \mod 1000$, $11^4=121^2=14641\equiv641 \mod 1000$, $11^8\equiv641^2=410881\equiv881 \mod 1000$, $11^{16}\equiv881^2=776161\equiv161 \mod 1000$, $11^{32}\equiv161^2=25921\equiv921 \mod 1000$, $11^{64}\equiv921^2=848241\equiv241 \mod 1000$, $11^{128}\equiv241^2=58081\equiv81 \mod 1000$, $11^{256}\equiv81^2=$ $=6561\equiv561 \mod 1000$, $11^{512}\equiv561^2=314721\equiv721 \mod 1000$, $11^{1024}\equiv721^2=519841\equiv841 \mod 1000$. Επομένως $11^{1280}=11^{1024}\cdot11^{256}\equiv841\cdot561=471801\equiv801 \mod 1000$, $11^{1408}=11^{1280}\cdot11^{128}\equiv$ $\equiv801\cdot81=64881\equiv881 \mod 1000$, $11^{1472}=11^{1408}\cdot11^{64}\equiv881\cdot241=212321\equiv321 \mod 1000$, $11^{1488}=$ $=11^{1472}\cdot11^{16}\equiv321\cdot161=51681\equiv681 \mod 1000$ και τέλος $11^{1492}=11^{1488}\cdot11^4\equiv681\cdot641=436521\equiv$ $\equiv521 \mod 1000$. Άρα ο αριθμός 11^{1492} λήγει σε 521. ■

Άσκηση 70. Βρείτε το ψηφίο που λείπει: $1751922\cdot11012=192921x5064$.
1η Λύση: Από την πρόταση 2.15 έχουμε $1751922\equiv1+7+5+1+9+2+2=27\equiv0 \mod 9\Rightarrow$ $\Rightarrow1751922\cdot11012\equiv0 \mod 9$. Επίσης $192921x5064\equiv1+9+2+9+2+1+x+5+0+6+4=39+x\equiv3+x \mod 9$. Επομένως $x+3\equiv0 \mod 9\Leftrightarrow x\equiv-3\equiv6 \mod 9$. Επειδή από τα ψηφία 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 μόνον το 6 είναι ισοϋπόλοιπο modulo 9 με το 6, έπεται ότι $x=6$.
2η Λύση: Θα μπορούσαμε να δουλέψουμε modulo 11. Έχουμε $1751922\equiv2-2+9-1+5-7+1=7 \mod 11$, $11012\equiv2-1+0-1+1=1 \mod 11$ και $192921x5064\equiv4-6+0-5+x-1+2-9+2-9+1=x-21 \mod 11$. Επομένως $7\cdot1\equiv x-21 \mod 11\Leftrightarrow x\equiv28\equiv6 \mod 11$. Άρα $x=6$. ■

Άσκηση 71. Βρείτε το άγνωστο ψηφίο x στο δεκαδικό σύστημα, ώστε $3x65\cdot962x=36245655$.
Λύση: Θα δουλέψουμε modulo 9 και modulo 11. Έχουμε: $3x65\equiv3+x+6+5\equiv x+5 \mod 9$, $962x\equiv x+8\equiv x-1 \mod 9$ και $36245655\equiv3+6+2+4+5+6+5+5\equiv0 \mod 9$. Επομένως $(x+5)(x-1)\equiv0 \mod 9\Leftrightarrow x^2+4x-5\equiv0 \mod 9\Leftrightarrow x^2+4x+4\equiv0 \mod 9\Leftrightarrow(x+2)^2\equiv0 \mod 9$. Παρατηρούμε ότι $(0+2)^2\equiv4 \mod 9$, $(1+2)^2=9\equiv0 \mod 9$, $(2+2)^2=16\equiv7 \mod 9$, $(3+2)^2=25\equiv7 \mod 9$, $(4+2)^2=36\equiv0 \mod 9$, $(5+2)^2=49\equiv4 \mod 9$, $(6+2)^2=64\equiv1 \mod 9$, $(7+2)^2=81\equiv0 \mod 9$, $(8+2)^2=100\equiv1 \mod 9$, $(9+2)^2\equiv2^2=4 \mod 9$. Πιθανά ψηφία τα 1, 4 και 7.
Τώρα δουλεύουμε modulo 11. Παρατηρούμε ότι $3x65\equiv5-6+x-3=x-4 \mod 11$, $962x\equiv x-2+6-9=$ $x-5 \mod 11$ και $36245655\equiv5-5+6-5+4-2+6-3=6 \mod 11$. Επομένως $(x-4)(x-5)\equiv6 \mod 11\Leftrightarrow x^2-9x+20-6\equiv0 \mod 11\Leftrightarrow x^2+2x+3\equiv0 \mod 11$. Για $x=1$ παίρνουμε $1^2+2\cdot1+3=6 \mod 11$, για $x=4$ παίρνουμε $4^2+2\cdot4+3=16+8+3\equiv16\equiv5 \mod 11$ και τέλος, για $x=7$ παίρνουμε παίρνουμε $7^2+2\cdot7+3=49+14+3\equiv5+3+3=11\equiv0 \mod 11$. Άρα $x=7$. ■

Άσκηση 72. Έστω $(xy)_{10}$ και $(yx)_{10}$ δύο διψήφιοι αριθμοί στο δεκαδικό σύστημα. Δείξτε ότι το άθροισμά τους είναι σύνθετος.
Απόδειξη: $(xy)_{10} = 10x + y$ και $(yx)_{10} = 10y + x$. Εφόσον οι αριθμοί είναι διψήφιοι, κανείς από τους x, y δεν είναι μηδέν. Τώρα, $(xy)_{10} + (yx)_{10} = 10(x+y) + (x+y) = 11(x+y)$. Αλλά $x + y \geq 1 + 1 = 2$, οπότε ο $11(x+y)$ είναι σύνθετος. ■

Άσκηση 73. Βρείτε τις τιμές του θετικού ακεραίου n, για τον οποίο το άθροισμα $1! + 2! + 3! + 4! + \cdots + n!$ είναι γνήσια δύναμη ακεραίου, δηλαδή της μορφής α^k, όπου $k \geq 2$.
Λύση: Παρατηρούμε ότι $1! = 1^k$, για οποιονδήποτε $k \geq 2$. Επίσης, $1! + 2! = 3$, $1! + 2! + 3! = 9 = 3^2$. Θα αποδείξουμε ότι το 1 και το 3 είναι οι μοναδικές λύσεις της άσκησης. Έχουμε $1! + 2! + 3! + 4! = 33 = 3 \cdot 11$, $1! + 2! + 3! + 4! + 5! = 153 = 9 \cdot 17$.
Παρατήρηση 1η: Επειδή $n! \equiv 0 \mod 10$, για κάθε $n \geq 5$ και ο αριθμός $1! + 2! + 3! + 4! = 33$ λήγει σε 3, κάθε άθροισμα $1! + 2! + 3! + 4! + 5! + \cdots + n!$, όπου $n \geq 5$, έχει τελευταίο ψηφίο το 3.
Τώρα, $1! + 2! + 3! + 4! + 5! + 6! = 873 = 3^2 \cdot 97$, $1! + 2! + 3! + 4! + 5! + 6! + 7! = 5913 = 3^4 \cdot 73$ και $1! + 2! + 3! + 4! + 5! + 6! + 7! + 8! = 46233 = 3^2 \cdot 5137 = 3^2 \cdot 11 \cdot 467$.
Παρατήρηση 2η: Επειδή οι αριθμοί 3, 11, 17, 73, 97 και 467 είναι πρώτοι, κανείς από τους αριθμούς 2, 4, 5, 6, 7 και 8 δεν είναι λύση του προβλήματος. Άρα το n, αν υπάρχει τέτοιο, θα πρέπει να είναι μεγαλύτερο ή ίσο του 9.
Παρατήρηση 3η: Επειδή $3^3 \mid n!$, για κάθε $n \geq 9$ και $3^2 \mid 1! + 2! + 3! + 4! + 5! + 6! + 7! + 8!$, αν το $1! + 2! + 3! + \cdots + n!$, όπου $n \geq 9$, ήταν της μορφής α^k με $k \geq 3$, τότε το 3^k, άρα και το 3^3 θα διαιρούσε το $1! + 2! + 3! + 4! + 5! + 6! + 7! + 8! + 9! + \cdots + n!$. Επειδή $3^3 \mid 9! + 10! + \cdots + n!$, θα έπρεπε $3^3 \mid 1! + 2! + 3! + 4! + 5! + 6! + 7! + 8! = 3^2 \cdot 11 \cdot 467$, άτοπο. Επομένως θα πρέπει $k = 2$, δηλαδή το $1! + 2! + 3! + 4! + \cdots + n!$ να είναι τέλειο τετράγωνο.
Έστω $1! + 2! + 3! + 4! + \cdots + n! = \alpha^2$, όπου $\alpha > 0$ και $n \geq 9$. Σύμφωνα με την πρώτη παρατήρηση, θα πρέπει $\alpha^2 \equiv 3 \mod 10$. Έστω x το τελευταίο ψηφίο του α. Τότε $\alpha \equiv x \mod 10 \Rightarrow \alpha^2 \equiv x^2 \mod 10$, δηλαδή $x^2 \equiv 3 \mod 10$. Παρατηρούμε όμως ότι $0^2 \equiv 0 \mod 10$, $1^2 \equiv 1 \mod 10$, $2^2 \equiv 4 \mod 10$, $3^2 \equiv 9 \mod 10$, $4^2 \equiv 6 \mod 10$, $5^2 \equiv 5 \mod 10$, $6^2 \equiv 6 \mod 10$, $7^2 \equiv 9 \mod 10$, $8^2 \equiv 4 \mod 10$ και $9^2 \equiv 1 \mod 10$. Συνεπώς δεν υπάρχει $n \geq 9$ που να είναι λύση του προβλήματος.
Οι μόνες λύσεις είναι λοιπόν το 1 και το 3. ■

Άσκηση 74. Αν $p > 3$ είναι πρώτος, δείξτε ότι $13 \mid 10^{2p} - 10^p + 1$.
Απόδειξη: Παρατηρούμε ότι $100 \equiv 9 \mod 13$. Άρα $10^{2p} \equiv 9^p \mod 13$. Επίσης $10 \equiv -3 \mod 13$. Επομένως $10^{2p} - 10^p + 1 \equiv 9^p - (-3)^p + 1 = 3^{2p} + 3^p + 1 \mod 13$, γιατί το p είναι περιττός.
Τώρα, $3^3 = 27 \equiv 1 \mod 13$. Ισχυριζόμαστε ότι αν k είναι θετικός ακέραιος και $3^k \equiv 1 \mod 13$, τότε $3 \mid k$. Πράγματι, έστω $k = 3\lambda + \upsilon$, όπου $0 \leq \upsilon < 3$. Αν $\upsilon = 1$, τότε $3^k = 3^{3\lambda+1} = (3^3)^\lambda \cdot 3 \equiv 1 \cdot 3 = 3 \mod 13$. Αν $\upsilon = 2$, τότε $3^k = 3^{3\lambda+2} = (3^3)^\lambda \cdot 3^2 \equiv 1 \cdot 9 = 9 \mod 13$. Άρα $\upsilon = 0$, δηλαδή $3 \mid k$. Εφόσον $p > 3$ πρώτος, έπεται ότι $3 \nmid p$. Επομένως $3^p \not\equiv 1 \mod 13 \Leftrightarrow 13 \nmid 3^p - 1 \Leftrightarrow (13, 3^p - 1) = 1$. Παρατηρούμε τώρα ότι $(3^p - 1)(3^{2p} + 3^p + 1) = 3^{3p} - 1 = (3^3)^p - 1 \equiv 1 - 1 = 0 \mod 13$, δηλαδή $13 \mid (3^p - 1)(3^{2p} + 3^p + 1)$. Επειδή $(13, 3^p - 1) = 1$, έπεται ότι $13 \mid 3^{2p} + 3^p + 1$. ■

Άσκηση 75. Γνωρίζουμε ότι η αρμονική σειρά $\sum_{n=1}^{\infty} \frac{1}{n}$ απειρίζεται θετικά. Αν από τη σειρά αυτή αφαιρέσουμε τους όρους $\frac{1}{n}$, όπου το 3 εμφανίζεται ως ψηφίο στη δεκαδική μορφή του n, θα πάρουμε τη σειρά $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{12} + \frac{1}{14} + \cdots + \frac{1}{22} + \frac{1}{24} + \cdots + \frac{1}{29} + \frac{1}{40} + \frac{1}{41} + \frac{1}{42} + \frac{1}{44} \cdots$ Αποδείξτε ότι η σειρά αυτή συγκλίνει.
Απόδειξη: Έστω A_κ το σύνολο των θετικών ακεραίων με κ ψηφία, διαφορετικά του 3. Αν $n \in \mathrm{A}_\kappa$, τότε $n \geq 10^{\kappa-1} \Leftrightarrow \frac{1}{n} \leq \frac{1}{10^{\kappa-1}}$. Πόσα είναι τα στοιχεία του A_κ; Για το 1ο ψηφίο έχουμε 8 επιλογές. (Τα ψηφία 0 και 3 απορρίπτονται). Για κάθε ένα από τα επόμενα $\kappa - 1$ ψηφία έχουμε 9 επιλογές. (Το ψηφίο 3 απορρίπτεται). Συνολικά έχουμε $8 \cdot 9^{\kappa-1}$ επιλογές. Άρα το σύνολο A_κ περιέχει $8 \cdot 9^{\kappa-1}$ αριθμούς που ο καθένας είναι μεγαλύτερος ή ίσος του $10^{\kappa-1}$. Επομένως, το ζητούμενο άθροισμα είναι $\sum_{\kappa=1}^{\infty} \Big(\sum_{n \in \mathrm{A}_\kappa} \frac{1}{n} \Big) \leq \sum_{\kappa=0}^{\infty} \frac{8 \cdot 9^{\kappa-1}}{10^{\kappa-1}} =$

$= 8 \cdot \sum_{\kappa=0}^{\infty} \left(\frac{9}{10}\right)^{\kappa} = 80$, δηλαδή άνω φραγμένο. Η αντίστοιχη λοιπόν σειρά συγκλίνει. ■

ΑΛΥΤΕΣ ΑΣΚΗΣΕΙΣ

64. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύουν οι σχέσεις:
(i) $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$.
(ii) $27 \mid 2^{5n+1} + 5^{n+2}$.
(iii) $11 \mid 5^{2n+1} + 2^{8n+9}$.
(iv) $7 \mid 3^{2n+5} + 2^{4n+1}$.
(v) $17 \mid 5^{2n+1} + 3 \cdot 2^{3n+2}$.

65. Έστω p πρώτος με $n < p < 2n$. Δείξτε ότι $\binom{2n}{n} \equiv 0 \mod p$.

66. Δείξτε ότι $\frac{3^{999} - 1}{2} \equiv 13 \mod 26$.

67. Βρείτε το υπόλοιπο της διαίρεσης 4444^{4444} δια 9.

68. Δείξτε ότι αν το $n > 0$ είναι περιττός, τότε το 229 διαιρεί τον αριθμό $13^{2n} + 17^{2n}$. Ισχύει το ίδιο αν το n είναι άρτιος;

69. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύει η σχέση: $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \mod 181$.

70. Βρείτε τα τρία τελευταία ψηφία του 7^{999}.

71. Βρείτε τα υπόλοιπα των παρακάτω διαιρέσεων:
(i) $17^{17} : 7$ **(ii)** $4^{30} : 23$ **(iii)** $3^{40} : 11$ **(iv)** $43^{37} : 11$ **(v)** $26^{1000} : 29$ **(vi)** $1! + 2! + 3! + \cdots + 500! : 189$
(vii) $3^{500} : 13$ **(viii)** $12! : 13$ **(ix)** $5^{16} : 17$ **(x)** $5^{500} : 17$.

72. Δείξτε ότι: **(i)** $97 \mid 2^{48} - 1$, **(ii)** $47 \mid 5^{23} + 1$ και **(iii)** $89 \mid 2^{44} - 1$.

73. Το άθροισμα των ψηφίων ενός αριθμού είναι 15. Δείξτε ότι ο αριθμός αυτός δεν τέλειο τετράγωνο ή τέλειος κύβος.

74. Βρείτε το άγνωστο ψηφίο x στο δεκαδικό σύστημα στις παρακάτω περιπτώσεις:
(i) $51840 \cdot 273581 = 1418243x040$.
(ii) $2x99561 = \big(3(523 + x)\big)^2$.
(iii) $2784x = x \cdot 5569$.
(iv) $512 \cdot 1x53125 = 10^9$.

75. Υποθέτουμε ότι το 495 διαιρεί τον αριθμό $273x49y5$. Βρείτε τα ψηφία x και y.

76. Αν $\alpha, \beta \in \mathbb{Z}$ με $\alpha \neq \beta$ και n θετικός ακέραιος, δείξτε ότι $\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}, \alpha - \beta\right) = (n(\alpha, \beta)^{n-1}, \alpha - \beta)$.

77. Αν n, N είναι θετικοί ακέραιοι, δείξτε ότι το 2^n διαιρεί τον N αν και μόνον αν το 2^n διαιρεί τον ακέραιο που σχηματίζεται από τα τελευταία n ψηφία του N.

2.3 Η συνάρτηση φ του Euler

Ορισμός 2.16. Έστω n θετικός ακέραιος. Ορίζουμε τη συνάρτηση $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+$ με
$$\varphi(n) = \text{το πλήθος των αριθμών } k \in \{1, 2, \ldots, n\} \text{ με } (k, n) = 1.$$
Η συνάρτηση φ λέγεται **συνάρτηση του Euler**.

Θεώρημα 2.17. Έστω n θετικός ακέραιος. Αν $n=1$, τότε $\varphi(n)=\varphi(1)=1$.
Αν $n>1$ και $n=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$ η ανάλυση του n σε γινόμενο πρώτων παραγόντων ($p_i\neq p_j$ για $i\neq j$ και $r_i>0$, για κάθε $i=1,2,\ldots,k$), τότε

$$\varphi(n)=n\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\cdots\Big(1-\frac{1}{p_k}\Big)=(p_1^{r_1}-p_1^{r_1-1})(p_1^{r_1}-p_2^{r_2-1})\cdots(p_k^{r_k}-p_k^{r_k-1})$$

Απόδειξη: Θα εφαρμόσουμε την αρχή του αποκλεισμού. (Βλέπε πόρισμα Δ΄.6-Παράρτημα Δ΄). Έστω A_i το σύνολο των ακεραίων από 1 έως n που διαιρούνται με το p_i, για κάθε $i=1,2,\ldots,k$. Ένας αριθμός $\kappa\in\{1,2,\ldots,n\}$ είναι πρώτος προς τον n αν και μόνον αν δεν έχει με τον n κοινό πρώτο διαιρέτη, δηλαδή δεν ανήκει σε κανένα από τα σύνολα $\mathrm{A}_1,\mathrm{A}_2,\ldots,\mathrm{A}_k$. Σύμφωνα με την αρχή του αποκλεισμού, $\varphi(n)=n-|\mathrm{A}_1\cup\mathrm{A}_2\cup\cdots\cup\mathrm{A}_k|$. (Εδώ το Ω είναι το σύνολο $\{1,2,\ldots,n\}$). Έχουμε $t\in\mathrm{A}_i\Leftrightarrow 1\leq t\leq n$ και $p_i\mid t$. Άρα, θέτοντας $t=s\cdot p_i$, έχουμε: $0<s\cdot p_i\leq n\Leftrightarrow 0<s\leq\dfrac{n}{p_i}$. Επομένως $|\mathrm{A}_i|=\dfrac{n}{p_i}$, για κάθε $i=1,2,\ldots,k$. Γενικότερα, ένας αριθμός από το σύνολο $\{1,2,\ldots,n\}$ ανήκει στην τομή $\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}\cap\cdots\mathrm{A}_{i_\lambda}$, δηλαδή ανήκει σε κάθε ένα από τα σύνολα $\mathrm{A}_{i_1},\mathrm{A}_{i_2},\ldots,\mathrm{A}_{i_\lambda}$, όπου $1\leq i_1<i_2<\cdots<i_\lambda\leq n$, αν και μόνον αν διαιρείται με κάθε p_{i_j}, για κάθε $j=1,2,\ldots,\lambda$. Επειδή τα p_i είναι διαφορετικοί πρώτοι, αυτό είναι ισοδύναμο με το να διαιρείται από το γινόμενο $p_{i_1}p_{i_2}\cdots p_{i_\lambda}$, δηλαδή να είναι της μορφής $s\cdot p_{i_1}p_{i_2}\cdots p_{i_\lambda}$. Τώρα, $0<s\cdot p_{i_1}p_{i_2}\cdots p_{i_\lambda}\leq n\Leftrightarrow 0<s\leq\dfrac{n}{p_{i_1}p_{i_2}\cdots p_{i_\lambda}}$. Επομένως $|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}\cap\cdots\mathrm{A}_{i_\lambda}|=\dfrac{n}{p_{i_1}p_{i_2}\cdots p_{i_\lambda}}$. Σύμφωνα με την αρχή του αποκλεισμού έχουμε:

$$\varphi(n)=n-|\mathrm{A}_1\cup\mathrm{A}_2\cup\cdots\cup\mathrm{A}_k|=n-\sum_{i=1}^{k}|\mathrm{A}_i|+\sum_{1\leq i_1<i_2\leq k}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}|-\sum_{1\leq i_1<i_2<i_3\leq k}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}\cap\mathrm{A}_{i_3}|+\cdots+$$

$$+(-1)^{k-1}\sum_{1\leq i_1<i_2<\cdots<i_{k-1}\leq n}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}\cap\cdots\cap\mathrm{A}_{i_{k-1}}|+(-1)^k|\mathrm{A}_1\cap\mathrm{A}_2\cap\cdots\cap\mathrm{A}_k|=n-\sum_{i=1}^{k}\frac{n}{p_i}+\sum_{1\leq i_1<i_2\leq k}\frac{n}{p_{i_1}p_{i_2}}-$$

$$-\sum_{1\leq i_1<i_2<i_3\leq k}\frac{n}{p_{i_1}p_{i_2}p_{i_3}}+\cdots+(-1)^{k-1}\sum_{1\leq i_1<i_2\cdots<i_{k-1}}\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_{k-1}}}+(-1)^k\frac{n}{p_1p_2\cdots p_k}=$$

$$=n\Bigg(1-\sum_{i=1}^{k}\frac{1}{p_i}+\sum_{1\leq i_1<i_2\leq k}\frac{1}{p_{i_1}p_{i_2}}-\sum_{1\leq i_1<i_2<i_3\leq k}\frac{1}{p_{i_1}p_{i_2}p_{i_3}}+\cdots+(-1)^{k-1}\sum_{1\leq i_1<i_2\cdots<i_{k-1}}\frac{1}{p_{i_1}p_{i_2}\cdots p_{i_{k-1}}}+$$

$$+(-1)^k\frac{1}{p_1p_2\cdots p_k}\Bigg).$$

Η παρένθεση ισούται με το γινόμενο $\Big(1-\dfrac{1}{p_1}\Big)\Big(1-\dfrac{1}{p_2}\Big)\cdots\Big(1-\dfrac{1}{p_k}\Big)$, αν κάνουμε τους πολλαπλασιασμούς σύμφωνα με την επιμεριστική ιδιότητα.
Τώρα, $\varphi(n)=n\Big(1-\dfrac{1}{p_1}\Big)\Big(1-\dfrac{1}{p_2}\Big)\cdots\Big(1-\dfrac{1}{p_k}\Big)=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}\Big(1-\dfrac{1}{p_1}\Big)\Big(1-\dfrac{1}{p_2}\Big)\cdots\Big(1-\dfrac{1}{p_k}\Big)=$
$=p_1^{r_1}\Big(1-\dfrac{1}{p_1}\Big)p_2^{r_2}\Big(1-\dfrac{1}{p_2}\Big)\cdots p_k^{r_k}\Big(1-\dfrac{1}{p_k}\Big)=(p_1^{r_1}-p_1^{r_1-1})(p_1^{r_1}-p_2^{r_2-1})\cdots(p_k^{r_k}-p_k^{r_k-1})$. ■

Πρόταση 2.18. Έστω m,n θετικοί ακέραιοι, με $(m,n)=1$. Τότε ισχύει

$$\varphi(mn)=\varphi(m)\varphi(n).$$

Απόδειξη: Αν $m=1$ ή $n=1$, τότε η πρόταση ισχύει γιατί $\varphi(1)=1$. Έστω $m,n>1$ και $m=p_1^{r_1}p_2^{r_2}\cdots p_\kappa^{r_\kappa}$, $n=q_1^{s_1}q_2^{s_2}\cdots q_\lambda^{s_\lambda}$ είναι οι αναλύσεις των m και n σε γινόμενα πρώτων. ($p_i\neq p_j$ και $q_i\neq q_j$ για κάθε i,j με $i\neq j$). Επειδή $(m,n)=1$, έχουμε $p_i\neq q_j$, για κάθε $i=1,2,\ldots,\kappa$ και $j=1,2,\ldots,\lambda$. Επομένως η ανάλυση του mn σε γινόμενο πρώτων παραγόντων είναι η

$$mn=p_1^{r_1}p_2^{r_2}\cdots p_\kappa^{r_\kappa}q_1^{s_1}q_2^{s_2}\cdots q_\lambda^{s_\lambda}.$$

Συνεπώς $\varphi(mn)=(p_1^{r_1}-p_1^{r_1-1})(p_2^{r_2}-p_2^{r_2-1})\cdots(p_\kappa^{r_\kappa}-p_\kappa^{r_\kappa-1})\cdot(q_1^{s_1}-q_1^{s_1-1})(q_2^{s_2}-q_2^{s_2-1})\cdots(q_\lambda^{s_\lambda}-q_\lambda^{s_\lambda-1})=$
$=\varphi(m)\varphi(n)$. ■

Η συνάρτηση φ ουσιαστικά μετράει **το πλήθος των κλάσεων ισοδυναμίας modulo n, των οποίων τα στοιχεία (αντιπρόσωποι) είναι πρώτοι προς το n**. Πιο συγκεκριμένα, έχουμε την ακόλουθη πρόταση:

Πρόταση 2.19. Έστω $n>0$ και $\alpha\equiv\beta\mod n$. Τότε ισχύουν τα εξής:

(i) $(\alpha, n) = (\beta, n)$.
(ii) $(\alpha, n) = 1 \Leftrightarrow (\beta, n) = 1$.
Απόδειξη: (i) Εφόσον $\alpha \equiv \beta \mod n$, θα έχουμε $\alpha - \beta = kn$, για κάποιο $k \in \mathbb{Z}$, δηλαδή $\alpha = \beta + kn$. Τότε $(\alpha, n) = (\beta + kn, n) = (\beta, n)$.
(ii) Προκύπτει άμεσα από το προηγούμενο. ■

Επομένως **υπάρχουν τόσοι αριθμοί $(\varphi(n))$ από το σύνολο $\{1, 2, \ldots, n\}$ που είναι πρώτοι προς το n, όσες είναι και οι κλάσεις ισοδυναμίας modulo n των οποίων τα στοιχεία είναι πρώτα προς το n**. Οι κλάσεις αυτές λέγονται **πρώτες προς το n**.

Ορισμός 2.20. Έστω $\langle x_1\rangle, \langle x_2\rangle, \ldots, \langle x_{\varphi(n)}\rangle$ οι κλάσεις ισοδυναμίας με στοιχεία πρώτα προς το n. (Η επιλογή των αντιπροσώπων $x_1, x_2, \ldots, x_{\varphi(n)}$ είναι τυχαία). Λέμε ότι οι αριθμοί $x_1, x_2, \ldots, x_{\varphi(n)}$ αποτελούν ένα **πλήρες ανηγμένο σύστημα υπολοίπων modulo n**.

Λήμμα 2.21. Έστω n θετικός ακέραιος και α μη μηδενικός ακέραιος.
(i) Αν $(\alpha, n) = 1$, τότε ισχύει η ισοδυναμία: $\alpha x \equiv \alpha y \mod n \Leftrightarrow x \equiv y \mod n$.
(ii) Γενικότερα ισχύει η ισοδυναμία: $\alpha x \equiv \alpha y \mod n \Leftrightarrow x \equiv y \mod \dfrac{n}{(\alpha, n)}$.
Απόδειξη: (i) $\alpha x \equiv \alpha y \mod n \Leftrightarrow n \mid \alpha x - \alpha y = \alpha(x - y) \underset{(\alpha,n)=1}{\Leftrightarrow} n \mid x - y \Leftrightarrow x \equiv y \mod n$.
(ii) $\alpha x \equiv \alpha y \mod n \Leftrightarrow n \mid \alpha(x - y) \Leftrightarrow \dfrac{n}{(\alpha, n)} \;\Big|\; \dfrac{\alpha}{(\alpha, n)}(x - y) \underset{\left(\frac{n}{(\alpha,n)}, \frac{\alpha}{(\alpha,n)}\right)=1}{\Leftrightarrow} \dfrac{n}{(\alpha, n)} \;\Big|\; x - y \Leftrightarrow \Leftrightarrow x \equiv y \mod \dfrac{n}{(\alpha, n)}$. ■

Πόρισμα 2.22. Έστω n θετικός ακέραιος και $(\alpha, n) = 1$.
(i) Αν $\{x_1, x_2, \ldots, x_n\}$ είναι ένα πλήρες σύστημα υπολοίπων modulo n, τότε το σύνολο $\{\alpha x_1, \alpha x_2, \ldots, \alpha x_n\}$ είναι επίσης ένα πλήρες σύστημα υπολοίπων modulo n.
(ii) Αν $\{x_1, x_2, \ldots, x_{\varphi(n)}\}$ είναι ένα πλήρες ανηγμένο σύστημα υπολοίπων modulo n, τότε το σύνολο $\{\alpha x_1, \alpha x_2, \ldots, \alpha x_{\varphi(n)}\}$ είναι επίσης ένα πλήρες ανηγμένο σύστημα υπολοίπων modulo n.
Απόδειξη: (i) Από το (i) του προηγουμένου λήμματος προκύπτει ότι εφόσον $x_i \not\equiv x_j \mod n$, για κάθε $i, j \in \{1, 2, \ldots, n\}$ με $i \neq j$, θα έχουμε και $\alpha x_i \not\equiv \alpha x_j \mod n$ για κάθε $i, j \in \{1, 2, \ldots, n\}$ με $i \neq j$. Εφόσον λοιπόν οι αριθμοί $\alpha x_1, \alpha x_2, \ldots, \alpha x_n$ είναι ανά δύο ανισοϋπόλοιποι modulo n, αυτοί αποτελούν ένα πλήρες σύστημα υπολοίπων modulo n.
(ii) Ότι τα $\alpha x_1, \alpha x_2, \ldots, \alpha x_{\varphi(n)}$ είναι ανά δύο ανισοϋπόλοιπα modulo n προκύπτει όπως παραπάνω. Αρ-κεί να δείξουμε ότι είναι πρώτα προς το n. Αυτό είναι άμεσο, αφού $(\alpha, n) = 1$ και $(x_i, n) = 1$, για κάθε $i = 1, 2, \ldots, x_{\varphi(n)}$. ■

Από το προηγούμενο πόρισμα προκύπτει ότι αν $\{x_1, x_2, \ldots, x_n\}$ είναι ένα πλήρες σύστημα υπολοίπων modulo n και $(\alpha, n) = 1$, τότε κάθε αx_κ με $\kappa \in \{1, 2, \ldots, n\}$, είναι ισοδύναμο modulo n με ένα **μοναδικό** x_{i_κ}, όπου $i_\kappa \in \{1, 2, \ldots, n\}$. Επίσης, αν $\kappa \neq \lambda$, τότε $i_\kappa \neq i_\lambda$. Γιατί αν $i_\kappa = i_\lambda$, τότε $\alpha x_\kappa \equiv x_{i_\kappa} = x_{i_\lambda} \equiv \alpha x_\lambda \mod n$, άτοπο. Επομένως τα σύνολα $\{x_1, x_2, \ldots, x_n\}$ και $\{x_{i_1}, x_{i_2}, \ldots, x_{i_n}\}$ συμπίπτουν. Απλώς τα στοιχεία τους είναι γραμμένα με διαφορετική σειρά.
Για τον ίδιο λόγο αν $(\alpha, n) = 1$, τότε $\{x_1, x_2, \ldots, x_{\varphi(n)}\} = \{x_{i_1}, x_{i_2}, \ldots, x_{i_{\varphi(n)}}\}$, όπου $\{x_1, x_2, \ldots, x_{\varphi(n)}\}$ είναι ένα πλήρες ανηγμένο σύστημα modulo n και $\alpha x_\kappa \equiv x_{i_\kappa} \mod n$, για κάθε $\kappa \in \{1, 2, \ldots, \varphi(n)\}$.

Η προηγούμενη θεώρηση μας επιτρέπει να δώσουμε μια άλλη απόδειξη για τον τύπο της συνάρτησης φ. Ξεκινάμε με το ακόλουθο λήμμα:

Λήμμα 2.23. Έστω m, n θετικοί ακέραιοι, με $(m, n) = 1$. Αν $x_1, x_2, \ldots, x_{\varphi(n)}$ είναι ένα πλήρες ανηγμένο σύστημα υπολοίπων modulo n και $y_1, y_2, \ldots, y_{\varphi(m)}$ ένα πλήρες ανηγμένο σύστημα υπολοίπων modulo m, τότε το σύνολο

$$\mathrm{A} = \{x_i m + y_j n \mid i = 1, 2, \ldots, \varphi(n) \text{ και } j = 1, 2, \ldots, \varphi(m)\}$$

αποτελεί ένα πλήρες ανηγμένο σύστημα **διακεκριμένων** υπολοίπων modulo mn.

Απόδειξη: Κατ' αρχάς θα αποδείξουμε ότι οι αριθμοί $x_im + y_jn$ ανήκουν σε διαφορετικές κλάσεις ισοδυναμίας modulo mn, οι οποίες είναι πρώτες προς το mn.

1) Δύο οποιαδήποτε στοιχεία του A ανήκουν σε διαφορετικές κλάσεις ισοδυναμίας modulo mn. Έστω λοιπόν ότι $x_{i_1}m + y_{j_1}n \equiv x_{i_2}m + y_{j_2}n \mod mn$, όπου $i_1, i_2 \in \{1, 2, \ldots, \varphi(n)\}$ και $j_1, j_2 \in \{1, 2, \ldots, \varphi(m)\}$. Τότε $mn \mid (x_{i_1} - x_{i_2})m + (y_{j_1} - y_{j_2})n$. Επομένως $m \mid (x_{i_1} - x_{i_2})m + (y_{j_1} - y_{j_2})n \Leftrightarrow m \mid (y_{j_1} - y_{j_2})n \underset{(m,n)=1}{\Leftrightarrow} m \mid y_{j_1} - y_{j_2} \Leftrightarrow y_{j_1} \equiv y_{j_2} \mod m$. Επειδή τα $y_1, y_2, \ldots, y_{\varphi(m)}$ ανήκουν σε διαφορετικές κλάσεις ισοδυναμίας modulo n, έχουμε $j_1 = j_2$. Κάνοντας τα ίδια πράγματα για το n συμπεραίνουμε ότι και $i_1 = i_2$.

2) Έστω $\delta = (x_im + y_jn, mn)$, για κάποια i, j. Τότε, αν $\delta > 1$ θα υπάρχει πρώτος p με $p \mid \delta$. Άρα $p \mid mn \Rightarrow p \mid m$ ή $p \mid n$. Αν $p \mid m$, τότε επειδή $(m, n) = 1$, $p \nmid n$. Επίσης $p \mid x_im + y_jn \underset{p|m}{\Leftrightarrow} p \mid y_jn$. Αλλά $p \nmid y_j$ (γιατί $(y_j, m) = 1$) και $p \nmid n$. Άρα $p \nmid y_jn$, άτοπο. Συμμετρικά καταλήγουμε σε άτοπο αν υποθέσουμε ότι $p \mid n$. Άρα $(x_im + y_jn, mn) = 1$. (Πιο απλά, θα μπορούσαμε να αποδείξουμε το προηγούμενο βάσει των (ii) και (iv) της πρότασης 1.21. Έχουμε: $(x_im + y_jn, mn) \underset{(m,n)=1}{=} (x_im + y_jn, m)(x_im + y_jn, n) = (y_jn, m)(x_im, n) = 1$, γιατί $(y_j, m) = (n, m) = 1$ και $(x_i, n) = (m, n) = 1$).

3) Έστω $z \in \mathbb{Z}$ πρώτο προς το mn. Απομένει να δείξουμε ότι $z \equiv x_im + y_jn \mod mn$, για κατάλληλα $i \in \{1, 2, \ldots, \varphi(n)\}$ και $j \in \{1, 2, \ldots, \varphi(m)\}$. Εφόσον $(m, n) = 1$, υπάρχουν $x, y \in \mathbb{Z}$ τέτοια, ώστε $xm + yn = 1$. Άρα $z = z(xm + yn) = (zx)m + (zy)n$.

Από τη σχέση $xm + yn = 1$ είναι σαφές ότι $(x, n) = 1 = (y, m)$. Επίσης, επειδή $(z, mn) = 1$, θα έχουμε $(z, m) = (z, n) = 1$. Άρα $(zx, n) = (zy, m) = 1$. Κατά συνέπεια $zx \equiv x_i \mod n$ και $zy \equiv y_j \mod m$, για κατάλληλα $i \in \{1, 2, \ldots, \varphi(n)\}$ και $j \in \{1, 2, \ldots, \varphi(m)\}$, ήτοι $n \mid zx - x_i \Leftrightarrow mn \mid (zx)m - x_im$ και $m \mid zy - y_j \Leftrightarrow mn \mid (zy)n - y_jn$. Συνεπώς $mn \mid (zx)m + (zy)n - (x_im + y_jn) \Leftrightarrow z = (zx)m + (zy)n \equiv x_im + y_jn \mod mn$. ■

Από το προηγούμενο λήμμα και χωρίς να γνωρίζουμε τον τύπο της φ, μπορούμε να δώσουμε μια δεύτερη απόδειξη της πρότασης 2.18.

2η Απόδειξη της Πρότασης 2.18: Αν $(m, n) = 1$, τότε σύμφωνα με το προηγούμενο λήμμα το σύνολο $A = \{x_im + y_jn \mid i = 1, 2, \ldots, \varphi(n) \text{ και } j = 1, 2, \ldots, \varphi(m)\}$ περιέχει ακριβώς $\varphi(m)\varphi(n)$ στοιχεία, τα οποία αποτελούν ένα πλήρες ανηγμένο σύστημα υπολοίπων modulo mn. Επομένως $\varphi(mn) = \varphi(m)\varphi(n)$. ■

3η Απόδειξη της Πρότασης 2.18: Έστω m και n θετικοί ακέραιοι με $(m, n) = 1$. Θα δείξουμε ότι

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Θεωρούμε τους αριθμούς από το σύνολο $A = \{1, 2, 3, \ldots, mn-1, mn\}$. Ξέρουμε ότι το σύνολο $\{1, 2, \ldots, m\}$ περιέχει $\varphi(m)$ αριθμούς, πρώτους προς τον m. Έστω $\kappa_1 < \kappa_2 < \cdots < \kappa_{\varphi(m)}$ οι αριθμοί αυτοί. Προφανώς $\kappa_1 = 1$ και $\kappa_{\varphi(m)} \leq m$.

Για κάθε $i = 1, 2, \ldots, \varphi(m)$ θεωρούμε το σύνολο $A_i = \{\kappa_i, \kappa_i + m, \kappa_i + 2m, \ldots, \kappa_i + (n-1)m\}$. Προφανώς όλοι οι αριθμοί του A_i είναι ισοϋπόλοιποι modulo m. Παρατηρούμε επίσης ότι $1 \leq \kappa_i \leq m$ και επομένως, για κάθε $\lambda = 0, 1, \ldots, n-1$ θα έχουμε: $1 \leq \kappa_i \leq \kappa_i + \lambda m \leq \kappa_i + (n-1)m \leq m + (n-1)m = mn$, δηλαδή $A_i \subseteq A$. Επίσης $A_i \cap A_j = \varnothing$, για $i \neq j$. Θα αποδείξουμε κάτι ισχυρότερο: κάθε στοιχείο του A_i είναι ανισοϋπόλοιπο modulo mn με κάθε στοιχείο του A_j. Γιατί, αν $\kappa_i + \lambda m \equiv \kappa_j + \mu m \mod mn$, όπου $\lambda, \mu \in \{0, 1, \ldots, n-1\}$, δηλαδή $mn \mid \kappa_i + \lambda m - \kappa_j - \mu m = \kappa_i - \kappa_j + (\lambda - \mu)m$, τότε και $m \mid \kappa_i - \kappa_j + (\lambda - \mu)m \Leftrightarrow m \mid \kappa_i - \kappa_j \Leftrightarrow \kappa_i \equiv \kappa_j \mod m$, άτοπο.

Τώρα, κάθε A_i αποτελεί ένα πλήρες σύστημα υπολοίπων modulo n. Πράγματι, αν $\kappa_i + \lambda m \equiv \kappa_i + \mu m \mod n$, όπου $\lambda, \mu \in \{0, 1, \ldots, n-1\}$, τότε $(\lambda - \mu)m \equiv 0 \mod n \underset{(m,n)=1}{\Leftrightarrow} \lambda - \mu \equiv 0 \mod n \Leftrightarrow \lambda = \mu$. Επομένως κάθε A_i περιέχει ακριβώς $\varphi(n)$ στοιχεία $\kappa_i + \lambda_1 m, \kappa_i + \lambda_2 m, \ldots, \kappa_i + \lambda_{\varphi(n)} m$ πρώτα προς το n. Έστω $B_i \subseteq A_i$ το σύνολό τους. Επειδή αυτά είναι ισοϋπόλοιπα modulo m με το κ_i, θα είναι πρώτα και προς το m. Άρα τα στοιχεία αυτά είναι πρώτα προς το mn. Επειδή $A_i \cap A_j = \varnothing$ για $i \neq j$, έχουμε βρει $\varphi(m)\varphi(n)$ στοιχεία από το σύνολο $A = \{1, 2, 3, \ldots, mn\}$, πρώτα προς το mn. Αυτά είναι τα στοιχεία της (ξένης) ένωσης

$\mathrm{B}_1 \cup \mathrm{B}_2 \cup \cdots \cup \mathrm{B}_{\varphi(m)}$.
Αντιστρόφως, έστω $k \in \{1, 2, 3, \ldots, mn\}$ πρώτο προς το mn. Διαιρούμε το k με το m και παίρνουμε πηλίκο λ και υπόλοιπο υ, δηλαδή $k = \lambda m + \upsilon$. Επειδή $(k, mn) = 1$, θα έχουμε και $(k, m) = (k, n) = 1$. Άρα και $(\upsilon, m) = (k - \lambda m, m) = (k, m) = 1$. Επομένως το υ είναι ίσο με κάποιο κ_i, όπου $i \in \{1, 2, \ldots, \varphi(m)\}$, δηλαδή $k = \kappa_i + \lambda m$. Προφανώς $\lambda m < \lambda m + \kappa_i = k \leq mn \Rightarrow \lambda < \dfrac{mn}{m} = n$. Άρα το λ είναι κάποιος από τους αριθμούς $0, 1, 2, \ldots, n-1$, δηλαδή $k = \lambda m + \kappa_i \in \mathrm{A}_i$. Επειδή δε $(k, n) = 1$, το λ είναι κάποιο από τα $\lambda_1, \lambda_2, \ldots, \lambda_{\varphi(n)}$. Το συμπέρασμα είναι ότι οι $\varphi(m)\varphi(n)$ αριθμοί που είχαμε βρει προηγουμένως είναι όλοι οι αριθμοί από το σύνολο $\mathrm{A} = \{1, 2, 3, \ldots, mn\}$, οι οποίοι είναι πρώτοι προς το mn. ■

Πόρισμα 2.24. Έστω $n_1, n_2, \ldots, n_k$ θετικοί ακέραιοι, ανά δύο πρώτοι μεταξύ τους. Τότε
$$\varphi(n_1 n_2 \cdots n_k) = \varphi(n_1)\varphi(n_2)\cdots\varphi(n_k).$$
Απόδειξη: Εφαρμόζουμε επαγωγή επί του k. Για $k = 2$ το έχουμε αποδείξει.
Έστω $k > 2$. Επειδή $(n_1 n_2 \cdots n_{k-1}, n_k) = 1$, έχουμε $\varphi(n_1 n_2 \cdots n_{k-1} n_k) = \varphi(n_1 \cdots n_{k-1})\varphi(n_k) \underset{\substack{\text{επαγωγική}\\ \text{υπόθεση}}}{=}$
$= \varphi(n_1)\cdots\varphi(n_{k-1})\varphi(n_k)$ ■

Σαν πόρισμα παίρνουμε μια δεύτερη απόδειξη του τύπου της φ.

2η Απόδειξη του Θεωρήματος 2.17: Έστω $n > 1$ και $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ η ανάλυση του n σε γινόμενο πρώτων παραγόντων ($p_i \neq p_j$ για $i \neq j$ και $r_i > 0$, για κάθε $i = 1, 2, \ldots, k$). Επειδή $(p_i^{r_i}, p_j^{r_j}) = 1$ για $i \neq j$, θα έχουμε:
$$\varphi(n) = \varphi(p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}) = \varphi(p_1^{r_1})\varphi(p_2^{r_2})\cdots\varphi(p_k^{r_k}).$$
Τώρα, για κάθε $i = 1, 2, \ldots, k$ το πλήθος των αριθμών από το σύνολο $\{1, 2, \ldots, p_i^{r_i}\}$ που είναι πρώτοι προς το $p_i^{r_i}$ είναι ακριβώς αυτοί που δεν διαιρούνται με το p_i.
Αυτοί που διαιρούνται με το p_i είναι της μορφής $s \cdot p_i$, όπου s θετικός ακέραιος και $s \cdot p_i \leq p_i^{r_i} \Leftrightarrow 0 < s \leq$
$\leq \dfrac{p_i^{r_i}}{p_i} = p_i^{r_i - 1}$. Άρα οι πρώτοι προς το $p_i^{r_i}$ είναι $p_i^{r_i} - p^{r_i - 1}$ το πλήθος, δηλαδή $\varphi(p_i^{r_i}) = p_i^{r_i} - p^{r_i - 1}$. Επομένως
$$\varphi(n) = (p_1^{r_1} - p_1^{r_1 - 1})(p_2^{r_2} - p_2^{r_2 - 1})\cdots(p_\kappa^{r_\kappa} - p_\kappa^{r_\kappa - 1}).$$ ■

Άσκηση 76. Δείξτε ότι αν m, n είναι θετικοί ακέραιοι με $m \mid n$, τότε $\varphi(m) \mid \varphi(n)$.
Απόδειξη: Αν $m = 1$, τότε $\varphi(m) = \varphi(1) = 1 \mid \varphi(n)$. Υποθέτουμε λοιπόν ότι $m > 1$. Έστω $m =$
$= p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ η ανάλυση του m σε γινόμενο πρώτων παραγόντων. $\big(p_i \neq p_j$ για $i \neq j$ και $r_i > 0$, για κάθε $i = 1, 2, \ldots, k\big)$. Τότε $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} \cdot \lambda$, όπου $s_i \geq r_i$ και $(\lambda, p_i) = 1$, για κάθε $i = 1, 2, \ldots, k$. $\big($Πιθανόν $\lambda = 1\big)$. Τότε $\varphi(n) = \varphi(p_1^{s_1} \cdots p_k^{s_k})\varphi(\lambda) = p_1^{s_1} \cdots p_k^{s_k}\left(1 - \dfrac{1}{p_1}\right)\cdots\left(1 - \dfrac{1}{p_k}\right)\varphi(\lambda) = p_1^{r_1} \cdots p_k^{r_k}$
$\left(1 - \dfrac{1}{p_1}\right)\cdots\left(1 - \dfrac{1}{p_k}\right)p_1^{s_1 - r_1} \cdots p_k^{s_k - r_k}\varphi(\lambda) = \varphi(m) \cdot p_1^{s_1 - r_1} \cdots p_k^{s_k - r_k}\varphi(\lambda)$. ■

Άσκηση 77. Βρείτε όλους τους θετικούς ακεραίους n, για τους οποίους
(i) $\varphi(n) = \dfrac{n}{2}$, **(ii)** $\varphi(n) = \varphi(2n)$, **(iii)** $\varphi(n) = 12$ και **(iv)** $\varphi(3n) = \varphi(4n) = \varphi(6n)$.
Λύση: (i) Εφόσον $\dfrac{n}{2} = \varphi(n) \in \mathbb{Z}$, το n είναι άρτιος. Έστω $n = 2^r\lambda$, όπου $r \geq 1$ και λ περιττός. Ένας περιττός $\lambda > 1$ έχει λιγότερους από λ πρώτους προς αυτόν από το σύνολο $\{1, 2, \ldots, \lambda\}$. Αυτό, γιατί ο ίδιος ο λ δεν είναι πρώτος προς τον εαυτό του. Αν λοιπόν $\lambda > 1$, θα είχαμε $\varphi(2^r\lambda) = 2^{r-1}\varphi(\lambda) < 2^{r-1}\lambda = \dfrac{n}{2}$. Επομένως $\lambda = 1$ και άρα ο n είναι δύναμη του 2, δηλαδή $n = 2^r$, όπου $r > 0$.
(ii) Αν ο n ήταν άρτιος της μορφής $n = 2^r\lambda$, όπου $r \geq 1$ και λ περιττός, τότε $\varphi(2n) = \varphi(2^{r+1}\lambda) = 2^r\varphi(\lambda) =$
$= 2 \cdot 2^{r-1}\varphi(\lambda) = 2\varphi(n)$. Επομένως ο n είναι περιττός. Τότε $(n, 2) = 1$ και άρα $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$.
(iii) Κατ' αρχάς ο n δεν μπορεί να είναι δύναμη του 2, γιατί $\varphi(2^r) = 2^{r-1}$. Άρα ο n έχει περιττό πρώτο διαιρέτη. Αν το n είχε τρεις διαφορετικούς περιττούς πρώτους παράγοντες p_1, p_2, p_3, τότε $p_1p_2p_3 \mid n$ και άρα $\varphi(p_1p_2p_3) \mid \varphi(n) = 12 \Rightarrow \varphi(p_1)\varphi(p_2)\varphi(p_3) = (p_1 - 1)(p_2 - 1)(p_3 - 1) \mid 12$. Αλλά $2 \mid p_i - 1 = \varphi(p_i)$, για κάθε $i = 1, 2, 3$. Επομένως $2^3 = 8 \mid 12$, άτοπο. Άρα το n έχει το πολύ δύο περιττούς πρώτους παράγοντες.

Έστω ότι έχει ακριβώς δύο και αυτοί να είναι οι p_1 και p_2 με $p_1 < p_2$. Ο p_2 θα είναι λοιπόν μεγαλύτερος του 3. $\big($Ο ελάχιστος περιττός πρώτος$\big)$. Ο $\varphi(p_2) = p_2 - 1$ δεν μπορεί λοιπόν να είναι 2. Αλλά ούτε να διαιρείται με το 4, γιατί τότε $8 \mid (p_1 - 1)(p_2 - 1) = \varphi(p_1 p_2) \mid 12$. Άρα διαιρείται με έναν περιττό πρώτο, ο οποίος αναγκαστικά θα είναι ο 3. $\big(12 = 2^2 \cdot 3\big)$. Συνοψίζοντας, ο $p_1 - 1$ διαιρείται με το 2, ο $p_2 - 1$ με το $6 = 2 \cdot 3$ και δεν πρέπει να εμφανίζεται άλλος πρώτος διαιρέτης, αφού $2 \cdot 6 = 12$. Αν κάποιος από τους p_1, p_2 ήταν υψωμένος σε μια γνήσια δύναμη (εκθέτης μεγαλύτερος του 1), αυτός θα διαιρούσε το 12, άρα θα ήταν ο 3. Επομένως ο 3 θα εμφανιζόταν δύο φορές, δηλαδή $3^2 \mid 12$, άτοπο. Συμπέρασμα: $p_1 - 1 = 2 \Leftrightarrow p_1 = 3$ και $p_2 - 1 = 6 \Leftrightarrow p_2 = 7$. Επειδή $(2, p_1 p_2) = 1$ και $\varphi(2) = 1$, οι δυνατές τιμές για τον n είναι $3 \cdot 7 = \mathbf{21}$ και $2 \cdot 3 \cdot 7 = \mathbf{42}$.

Απομένει η περίπτωση κατά την οποία ο n έχει έναν μόνον περιττό πρώτο παράγοντα p. Αν $p^2 \mid n$, τότε $p(p-1) = p^2 - p = \varphi(p^2) \mid \varphi(n) = 12$ και άρα $p \mid 12 = 2^2 \cdot 3$. Επομένως $p = 3$. Αλλά $\varphi(3^2) = 6 \neq 12$ και $9 \mid \varphi(3^k) = 3^{k-1} \cdot 2$, για κάθε $k \geq 3$. Συμπέρασμα: Ο p δεν είναι υψωμένος σε γνήσια δύναμη και δεν είναι ο 3. Επίσης ο n δεν μπορεί να διαιρείται με το $2^3 = 8$, γιατί τότε $\varphi(2^3) = 4$ και επίσης $2 \mid \varphi(p) = p - 1$. Επομένως θα είχαμε $8 = 4 \cdot 2 \mid \varphi(2^3)\varphi(p) = \varphi(2^3 \cdot p) \mid \varphi(n) = 12$, άτοπο. Άρα $n = 4p$ ή $n = 2p$ ή $n = p$. Στην πρώτη περίπτωση παίρνουμε $12 = \varphi(4)\varphi(p) = 2(p-1) \Leftrightarrow p - 1 = 6 \Leftrightarrow p = 7$. Άρα $n = 4 \cdot 7 = \mathbf{28}$. Στη δεύτερη περίπτωση παίρνουμε $12 = \varphi(2)\varphi(p) = p - 1$ και το ίδιο στην τρίτη $12 = \varphi(p) = p - 1$. Άρα $p - 1 = 12 \Leftrightarrow p = 13$. Οι δυνατές τιμές για το n είναι **13** και **26**. Οι λύσεις του προβλήματος είναι λοιπόν οι αριθμοί 13, 21, 26, 28 και 42.

(iv) Έστω $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ η ανάλυση του n σε γινόμενο πρώτων παραγόντων. Τότε

$$\varphi(n) = p_1^{r_1 - 1} p_2^{r_2 - 1} \cdots p_k^{r_k - 1}(p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

Αν κάποιος από τους p_i ήταν ο 2, τότε $\varphi(4n) = 4\varphi(n)$ και αν κάποιος από τους p_i ήταν ο 3, τότε $\varphi(3n) = 3\varphi(n)$. $\big($Αυξάνει η δύναμη στο αντίστοιχο $p_i^{r_i - 1}\big)$. Αν λοιπόν $3 \mid n$, τότε $2 \nmid n$, οπότε $\varphi(3n) = 3\varphi(n)$, ενώ $\varphi(4n) = \varphi(4)\varphi(n) = 2\varphi(n)$, άτοπο. Επομένως $3 \nmid n$. Πάλι, αν $2 \mid n$, τότε $3 \nmid n$, οπότε $\varphi(4n) = 4\varphi(n)$, ενώ $\varphi(3n) = \varphi(3)\varphi(n) = 2\varphi(n)$, άτοπο. Άρα $2 \nmid n$ και $3 \nmid n$. Συμπεραίνουμε ότι $(2, n) = (3, n) = 1 \Leftrightarrow (6, n) = 1$. Άρα $\varphi(4n) = \varphi(4)\varphi(n) = 2\varphi(n)$, $\varphi(3n) = \varphi(3)\varphi(n) = 2\varphi(n)$ και $\varphi(6n) = \varphi(6)\varphi(n) = 2\varphi(n)$, δηλαδή $\varphi(4n) = \varphi(3n) = \varphi(6n)$. Ικανή και αναγκαία συνθήκη για να ισχύει η σχέση $\varphi(3n) = \varphi(4n) = \varphi(6n)$ είναι $(n, 6) = 1 \Leftrightarrow \big(2 \nmid n$ και $3 \nmid n\big)$. ■

Άσκηση 78. Έστω m, n θετικοί ακέραιοι και $d = (m, n)$. Τότε ισχύει η σχέση:

$$\varphi(mn)\varphi(d) = d\varphi(m)\varphi(n).$$

Απόδειξη: Για κάθε θετικό ακέραιο k ορίζουμε το σύνολο $\mathrm{A}_k = \{p \mid p$ πρώτος και $p \mid k\}$. Τότε το $\varphi(k)$ γράφεται

$$\varphi(k) = k \prod_{p \in \mathrm{A}_k} \Big(1 - \frac{1}{p}\Big).$$

Παρατηρούμε ότι $\mathrm{A}_m \cap \mathrm{A}_n = \{p \mid p$ πρώτος, $p \mid m$ και $p \mid n\} = \{p \mid p$ πρώτος και $p \mid (m, n) = d\} = \mathrm{A}_d$. Επίσης $\mathrm{A}_m \cup \mathrm{A}_n = \{p \mid p$ πρώτος και $p \mid m$ ή $p \mid n\} = \{p \mid p$ πρώτος και $p \mid mn\} = \mathrm{A}_{mn}$. Επομένως

$$\varphi(m)\varphi(n) = m \prod_{p \in \mathrm{A}_m} \Big(1 - \frac{1}{p}\Big) n \prod_{p \in \mathrm{A}_n} \Big(1 - \frac{1}{p}\Big) = mn \prod_{p \in \mathrm{A}_m \setminus \mathrm{A}_d} \Big(1 - \frac{1}{p}\Big) \prod_{p \in \mathrm{A}_n \setminus \mathrm{A}_d} \Big(1 - \frac{1}{p}\Big) \Big(\prod_{p \in \mathrm{A}_d} \Big(1 - \frac{1}{p}\Big)\Big)^2 =$$

$$= mn \prod_{p \in \mathrm{A}_m \setminus \mathrm{A}_d} \Big(1 - \frac{1}{p}\Big) \prod_{p \in \mathrm{A}_n \setminus \mathrm{A}_d} \Big(1 - \frac{1}{p}\Big) \prod_{p \in \mathrm{A}_d} \Big(1 - \frac{1}{p}\Big) \cdot d \prod_{p \in \mathrm{A}_d} \Big(1 - \frac{1}{p}\Big) \cdot \frac{1}{d} =$$

$$= mn \prod_{p \in \mathrm{A}_m \cup \mathrm{A}_n} \Big(1 - \frac{1}{p}\Big) \varphi(d) \cdot \frac{1}{d} = mn \prod_{p \in \mathrm{A}_{mn}} \Big(1 - \frac{1}{p}\Big) \varphi(d) \cdot \frac{1}{d} = \frac{\varphi(mn)\varphi(d)}{d}.$$

Επομένως $\varphi(m)\varphi(n)d = \varphi(mn)\varphi(d)$. ■

2.4 Τα Θεωρήματα των Euler, Fermat και Wilson

Θεώρημα 2.25. (Θεώρημα του Euler) Έστω n θετικός ακέραιος και $(\alpha, n) = 1$. Τότε $\alpha^{\varphi(n)} \equiv 1 \mod n$.

Απόδειξη: Έστω $\{x_1, x_2, \ldots, x_{\varphi(n)}\}$ ένα πλήρες ανηγμένο σύστημα αντιπροσώπων modulo n. Σύμφωνα με

τις προηγούμενες παρατηρήσεις έχουμε τις σχέσεις:

$$\begin{aligned}
\alpha x_1 &\equiv x_{i_1} \mod n \\
\alpha x_2 &\equiv x_{i_2} \mod n \\
\alpha x_3 &\equiv x_{i_3} \mod n \\
&\vdots \\
\alpha x_{\varphi(n)} &\equiv x_{i_{\varphi(n)}} \mod n
\end{aligned}$$

Αν πολλαπλασιάσουμε κατά μέλη τις ισοδυναμίες αυτές θα πάρουμε: $\alpha^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)} \equiv x_{i_1} x_{i_2} \cdots x_{i_{\varphi(n)}} = x_1 x_2 \cdots x_{\varphi(n)} \mod n$, επειδή τα σύνολα $\{x_1, x_2, \ldots, x_{\varphi(n)}\}$ και $\{x_{i_1}, x_{i_2}, \ldots, x_{i_{\varphi(n)}}\}$ συμπίπτουν. Επομένως $n \mid (\alpha^{\varphi(n)} - 1) x_1 x_2 \cdots x_{\varphi(n)}$. Επειδή $(x_1 x_2 \cdots x_{\varphi(n)}, n) = 1$, προκύπτει ότι $n \mid \alpha^{\varphi(n)} - 1 \Leftrightarrow \alpha^{\varphi(n)} \equiv 1 \mod n$. ■

Πόρισμα 2.26. («Μικρό» Θεώρημα του Fermat) Έστω p πρώτος και $\alpha \in \mathbb{Z}$ με $p \nmid \alpha$. Τότε ισχύει

$$\alpha^{p-1} \equiv 1 \mod p.$$

Απόδειξη: Ως γνωστόν ισχύει η ισοδυναμία $p \nmid \alpha \Leftrightarrow (\alpha, p) = 1$. Επίσης $\varphi(p) = p - 1$, αφού όλοι οι αριθμοί $1, 2, \ldots, p-1$ αποτελούν πλήρες ανηγμένο σύστημα υπολοίπων modulo p. Το αποτέλεσμα προκύπτει λοιπόν από το προηγούμενο θεώρημα του Euler. ■

Πόρισμα 2.27. Έστω p πρώτος και $\alpha \in \mathbb{Z}$. Τότε ισχύει η σχέση $\alpha^p \equiv \alpha \mod p$.
Απόδειξη: Αν $(\alpha, p) = 1$, τότε $\alpha^{p-1} \equiv 1 \mod p \Rightarrow \alpha^p \equiv \alpha \mod p$. Αν $(\alpha, p) \underset{p \text{ πρώτος}}{=} p$, τότε $p \mid \alpha$ και $p \mid \alpha^p$, άρα $\alpha^p \equiv \alpha \equiv 0 \mod p$. ■

Θεώρημα 2.28. (Θεώρημα του Wilson) Έστω $p > 1$. Τότε ο p είναι πρώτος αν και μόνον αν

$$(p-1)! \equiv -1 \mod p.$$

Απόδειξη: Αρχικώς θα αποδείξουμε ότι αν $(p-1)! \equiv -1 \mod p$, τότε ο p είναι πρώτος. Ας υποθέσουμε λοιπόν ότι ο p είναι σύνθετος και $(p-1)! \equiv -1 \mod p$. Ο p ως σύνθετος θα έχει έναν γνήσιο διαιρέτη n, δηλαδή $1 < n < p$. Τότε $n \leq p-1$ και επομένως $n \mid (p-1)!$. Εφόσον όμως $p \mid (p-1)! + 1$ και $n \mid p$, έπεται $n \mid (p-1)! + 1$. Επομένως θα ίσχυαν ταυτόχρονα οι σχέσεις $n \mid (p-1)!$ και $n \mid (p-1)! + 1$. Από αυτές προκύπτει ότι $n \mid (p-1)! + 1 - (p-1)! = 1$, δηλαδή $n = 1$, άτοπο.
Αντιστρόφως, υποθέτουμε ότι ο p είναι πρώτος. Θα δείξουμε ότι $p \mid (p-1)! + 1$. Για $p = 2$ η σχέση αυτή ισχύει. Επομένως μπορούμε να υποθέσουμε ότι ο p είναι περιττός.
Έστω $\alpha \in \{1, 2, \ldots, p-1\}$. Προφανώς $(\alpha, p) = 1$ και επειδή το σύνολο $\{1, 2, \ldots, p-1\}$ αποτελεί ένα πλήρες ανηγμένο σύστημα υπολοίπων modulo n, τότε και το σύνολο $\{\alpha \cdot 1, \alpha \cdot 2, \ldots, \alpha \cdot (p-1)\}$ αποτελεί και αυτό ένα πλήρες ανηγμένο σύστημα υπολοίπων modulo n. Επομένως υπάρχει μοναδικός $\alpha' \in \{1, 2, \ldots, p-1\}$ τέτοιος, ώστε $\alpha\alpha' \equiv 1 \mod p$. Ας ονομάσουμε τον α' **αντίστροφο του α modulo p**.
Ποιος είναι τώρα ο αντίστροφος του α' modulo p; Επειδή $\alpha\alpha' \equiv 1 \mod p \Leftrightarrow \alpha'\alpha \equiv 1 \mod p$, ο αντίστροφος $\alpha'' := (\alpha')'$ του α' modulo p αναγκαστικά είναι ο α. (Ο αντίστροφος modulo p εξ ορισμού είναι μοναδικός). Οι αριθμοί λοιπόν $1, 2, 3, \ldots, p-1$ χωρίζονται εν γένει σε ξένα ζευγάρια-δισύνολα $\{\alpha, \alpha'\}$ αντιστρόφων modulo p. Είναι δυνατόν κάποιος από τους $1, 2, \ldots, p-1$ να είναι αντίστροφος του εαυτού του; Δηλαδή $\alpha^2 \equiv 1 \mod p$; Αυτό είναι ισοδύναμο με τη σχέση $p \mid \alpha^2 - 1 = (\alpha - 1)(\alpha + 1) \Leftrightarrow \big(p \mid \alpha - 1$ ή $p \mid \alpha + 1\big) \Leftrightarrow \big(\alpha \equiv 1 \mod p$ ή $\alpha \equiv -1 \equiv p - 1 \mod p\big)$. Επειδή δε οι αριθμοί $1, 2, \ldots, p-1$ είναι ανισοϋπόλοιποι modulo p, οι δυνατές περιπτώσεις είναι δύο: $\alpha = 1$ και $\alpha = p - 1$.
Συμπερασματικά, οι αριθμοί $2, 3, \ldots, p-2$ χωρίζονται σε ξένα ζευγάρια αντιστρόφων και κατά συνέπεια το γινόμενό τους είναι ισοϋπόλοιπο 1 modulo p. Ο αριθμός 1 δεν αλλάζει το γινόμενο, άρα το $(p-2)!$ είναι ισοϋπόλοιπο modulo p με το 1. Επομένως $(p-1)! = (p-2)!(p-1) \equiv 1 \cdot (p-1) = p - 1 \equiv -1 \mod p$. ■

Πόρισμα 2.29. Έστω $p > 1$. Τότε ο p είναι πρώτος αν και μόνον αν $(p-2)! \equiv 1 \mod p$.
Απόδειξη: Η απόδειξη προκύπτει άμεσα από την απόδειξη του θεωρήματος του Wilson. Παρ' όλα αυτά ας δούμε τον ακόλουθο συλλογισμό. Ο p είναι πρώτος αν και μόνον αν $(p-1)! \equiv -1 \equiv p - 1$

$\mod p \Leftrightarrow p \mid (p-1)! - (p-1) = (p-1)((p-2)! - 1) \underset{(p,p-1)=1}{\Leftrightarrow} p \mid (p-2)! - 1 \Leftrightarrow (p-2)! \equiv 1 \mod p.$ ■

Σημείωση: Από το «μικρό» θεώρημα του Fermat προκύπτει ότι ο αντίστροφος modulo p ενός αριθμού α, όπου $(\alpha, n) = 1$ ανήκει στην κλάση $\big($δηλαδή είναι ισοϋπόλοιπος modulo $p\big)$ με το α^{p-2}.

Από το θεώρημα του Euler έχουμε $\alpha^{\varphi(n)} \equiv 1 \mod n$, για κάθε $\alpha \in \mathbb{Z}$ με $(\alpha, n) = 1$.

Ορισμός 2.30. Έστω n θετικός ακέραιος και $\alpha \in \mathbb{Z}$ με $(\alpha, n) = 1$. Ο μικρότερος θετικός ακέραιος k με την ιδιότητα $\alpha^k \equiv 1 \mod n$ ονομάζεται **τάξη του α modulo n**.

Πρόταση 2.31. Έστω $(\alpha, n) = 1$ και k η τάξη του α modulo n. Αν λ είναι ένας θετικός ακέραιος τέτοιος, ώστε $\alpha^\lambda \equiv 1 \mod n$, τότε $k \mid \lambda$.
Απόδειξη: Έστω $\lambda = k\pi + \upsilon$ η ταυτότητα της διαίρεσης $\lambda : k$. Τότε $0 \le \upsilon < k$. Υποθέτουμε ότι $\upsilon > 0$. Τότε θα έχουμε: $1 \equiv \alpha^\lambda = \alpha^{k\pi+\upsilon} = (\alpha^k)^\pi \alpha^\upsilon \underset{\alpha^k \equiv 1 \mod n}{\equiv} \alpha^\upsilon \mod n$. Αυτό όμως είναι άτοπο, γιατί ο k είναι ο ελάχιστος θετικός εκθέτης στον οποίο υψωμένο το α γίνεται ισοϋπόλοιπο 1 modulo n και $\upsilon < k$. ■

Ορισμός 2.32. Οι αριθμοί $M_n = 2^n - 1$, όπου $n = 1, 2, \ldots$ ονομάζονται **αριθμοί Mersenne**.

Η επόμενη πρόταση μας παρέχει μία ακόμη απόδειξη της απειρίας των πρώτων αριθμών.

Πρόταση 2.33. Έστω $M_p = 2^p - 1$ ένας αριθμός Mersenne, όπου p πρώτος. Τότε κάθε πρώτος διαιρέτης του M_p είναι μεγαλύτερος του p.
Απόδειξη: Έστω q πρώτος διαιρέτης του $M_p = 2^p - 1$. Τότε $2^p \equiv 1 \mod q$. Επομένως η τάξη του 2 modulo q είναι διαιρέτης του p και άρα θα είναι 1 ή p. Αν ήταν 1, τότε θα είχαμε $2 = 2^1 \equiv 1 \mod q \Leftrightarrow q \mid 2 - 1 = 1$, άτοπο. Επομένως η τάξη του 2 modulo q είναι p. Επίσης, επειδή ο $M_p = 2^p - 1$ είναι περιττός, ο διαιρέτης q αυτού είναι επίσης περιττός. Άρα $(2, q) = 1$. Από το «μικρό» θεώρημα του Fermat προκύπτει ότι $2^{q-1} \equiv 1 \mod q$. Επομένως η τάξη p του 2 $\big($modulo $q\big)$ διαιρεί τον $q - 1$ και επομένως $p \le q - 1 < q$. ■

Πόρισμα 2.34. Υπάρχουν άπειροι πρώτοι.
Απόδειξη: Άμεση από την πρόταση, αφού για κάθε πρώτο p υπάρχει πρώτος q μεγαλύτερος του p. $\big($Ένας πρώτος διαιρέτης του $M_p\big)$. ■

Πρόταση 2.35. Αν ένας αριθμός της μορφής $\alpha^n - 1$ είναι πρώτος, όπου $\alpha, n > 1$, τότε ο n είναι πρώτος και $\alpha = 2$.
Απόδειξη: Αν ο n ήταν σύνθετος της μορφής $n = \kappa\lambda$, όπου $\kappa, \lambda > 1$, τότε $\alpha^\kappa - 1 \mid \alpha^n - 1$ και $1 < \alpha^\kappa - 1 < \alpha^n - 1$. Άρα ο n είναι πρώτος. Αν πάλι $\alpha > 2$, τότε $\alpha^n - 1 = (\alpha - 1)(\alpha^{n-1} + \alpha^{n-2} + \cdots + \alpha + 1)$ και $\alpha - 1 > 1$. Άρα ο $\alpha^n - 1$ θα ήταν σύνθετος. Απομένει λοιπόν η περίπτωση $\alpha = 2$ και n πρώτος. ■

Η προηγούμενη πρόταση δεν μας εξασφαλίζει ότι ένας αριθμός Mersenne $M_p = 2^p - 1$, όπου p πρώτος είναι κατ' ανάγκην πρώτος. Παρατηρούμε ότι $M_2 = 2^2 - 1 = 3$, $M_3 = 2^3 - 1 = 7$, $M_5 = 2^5 - 1 = 31$, $M_7 = 2^7 - 1 = 127$ είναι όλοι πρώτοι. Αλλά ο $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ είναι σύνθετος.
Οι πρώτοι αριθμοί της μορφής $M_p = 2^p - 1$, όπου p πρώτος, λέγονται **πρώτοι αριθμοί του Mersenne**.

Άσκηση 79. Στην άσκηση 36 αποδείξαμε ότι υπάρχουν άπειροι πρώτοι της μορφής $4\lambda + 3$, όπου λ θετικός ακέραιος. Θα αποδείξουμε τώρα ότι υπάρχουν άπειροι πρώτοι της μορφής $4\lambda + 1$, $\lambda \in \mathbb{Z}_+$.
Απόδειξη: Θεωρούμε έναν θετικό ακέραιο $\mathrm{N} > 1$, οσονδήποτε μεγάλο. Αρκεί να αποδείξουμε ότι υπάρχει πρώτος της μορφής $4\lambda + 1$, μεγαλύτερος του N. Ο αριθμός $\mathrm{A} = (\mathrm{N}!)^2 + 1$ έχει έναν πρώτο διαιρέτη q. Θα δείξουμε ότι ο q έχει τις απαιτούμενες ιδιότητες. Πρώτα απ' όλα, ο q είναι μεγαλύτερος του N. Σε αντίθετη περίπτωση θα είχαμε $q \mid \mathrm{N}! \Rightarrow q \mid (\mathrm{N}!)^2$. Αλλά $q \mid (\mathrm{N}!)^2 + 1$, οπότε θα είχαμε $q \mid (\mathrm{N}!)^2 + 1 - (\mathrm{N}!)^2 = 1$, άτοπο. Εφόσον $q \mid (\mathrm{N}!)^2 + 1$, έχουμε $(\mathrm{N}!)^2 \equiv -1 \mod q$. Επίσης, επειδή $q > \mathrm{N} > 1$, ο q είναι περιττός. Άρα ο $q - 1$ άρτιος, δηλαδή $\dfrac{q-1}{2} \in \mathbb{Z}_+$. Επομένως από τη σχέση $(\mathrm{N}!)^2 \equiv -1 \mod q$ έπεται ότι $(\mathrm{N}!)^{q-1} = \big((\mathrm{N}!)^2\big)^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{2}} \mod q$.

Απ' την άλλη μεριά, αφού $\mathrm{N} < q$, έχουμε $(\mathrm{N}!, q) = 1$. Από το «μικρό» θεώρημα του Fermat προκύπτει ότι $(\mathrm{N}!)^{q-1} \equiv 1 \mod q$. Επομένως $(-1)^{\frac{q-1}{2}} \equiv (\mathrm{N}!)^{q-1} \equiv 1 \mod q$. Επειδή το $(-1)^{\frac{q-1}{2}}$ ισούται με ± 1 και $-1 \not\equiv 1 \mod q \Leftrightarrow q \nmid 2$, πρέπει $(-1)^{\frac{q-1}{2}} = 1$, δηλαδή ο $\dfrac{q-1}{2}$ να είναι άρτιος. Έστω $\dfrac{q-1}{2} = 2\lambda$, για κάποιον θετικό ακέραιο λ. Τότε $q = 4\lambda + 1$ που είναι και το ζητούμενο. ■

Στις ασκήσεις 36 και 79 αποδείξαμε ότι υπάρχουν άπειροι πρώτοι της μορφής $4\lambda + 1$ και $4\lambda + 3$. Δεν είναι τυχαίο ότι $(1, 4) = (3, 4) = 1$. Ισχύει ένα γενικότερο αποτέλεσμα, το οποίο οφείλεται στον Dirichlet.

Θεώρημα 2.36. (Θεώρημα του Dirichlet) Αν α, β είναι θετικοί ακέραιοι με $(\alpha, \beta) = 1$, τότε υπάρχουν άπειροι πρώτοι που είναι όροι της αριθμητικής προόδου $\alpha, \alpha + \beta, \alpha + 2\beta, \alpha + 3\beta, \alpha + 4\beta, \ldots$ ■

Η απόδειξη του θεωρήματος του Dirichlet χρησιμοποιεί στοιχεία Μαθηματικής Ανάλυσης και θεωρίας χαρακτήρων αβελιανών ομάδων.

ΛΥΜΕΝΕΣ ΑΣΚΗΣΕΙΣ

Άσκηση 80. Δείξτε ότι υπάρχουν άπειροι σύνθετοι αριθμοί της μορφής $n! + 1$, όπου n θετικός ακέραιος.
Απόδειξη: Αν p είναι αρκούντως μεγάλος πρώτος, θα δείξουμε ότι $(p-1)! + 1 > p$. Γενικά, έστω m θετικός ακέραιος, με $m \geq 4$. Αν $m = 4$, τότε $(m-1)! + 1 = 3! + 1 = 7 > 4 = m$. Έστω ότι $(m-1)! + 1 > m$, για κάποιον θετικό ακέραιο $m \geq 4$. Τότε $(m+1-1)! + 1 = m! + 1 = (m-1)!m + 1 \underset{(m-1)! \geq 3! = 6}{\geq} 6m + 1 > m + 1$.
Επομένως $(m-1)! + 1 > m$, για κάθε $m \geq 4$.
Στην ειδική περίπτωση που $m = p \geq 5$ πρώτος, παίρνουμε $(p-1)! + 1 > p$. Βάσει του θεωρήματος του Wilson ο $(p-1)! + 1$ έχει έναν γνήσιο διαιρέτη p, άρα είναι σύνθετος. Επειδή υπάρχουν άπειροι πρώτοι, υπάρχουν και άπειροι σύνθετοι της μορφής $n! + 1$, όπου $n = p - 1$, με $p \geq 5$ πρώτο. ■

Άσκηση 81. Βρείτε τα υπόλοιπα των διαιρέσεων **(i)** $15! : 17$ και **(ii)** $2 \cdot 26! : 29$.
Λύση: (i) Από το πόρισμα 2.29 παίρνουμε $15! \equiv 1 \mod 17$.
(ii) Πάλι από το πόρισμα 2.29 παίρνουμε $27! \equiv 1 \mod 29 \Leftrightarrow 26! \cdot 27 \equiv 1 \mod 29$. Αλλά $27 \equiv -2 \mod 29$. Επομένως $-2 \cdot 26! \equiv 1 \mod 29 \Leftrightarrow 2 \cdot 26! \equiv -1 \equiv 28 \mod 29$. ■

Άσκηση 82. Δείξτε ότι $31 \mid 4 \cdot 29! + 5!$.
Απόδειξη: Ξέρουμε ότι, εφόσον ο 31 είναι πρώτος, $29! \equiv 1 \mod 31$. Επομένως $4 \cdot 29! + 5! \equiv 4 + 5! = 4 + 4! \cdot 5 = 4 + 24 \cdot 5 \equiv 4 + (-7) \cdot 5 = 4 - 35 = -31 \equiv 0 \mod 31$. ■

Άσκηση 83. Έστω p, q δύο διαφορετικοί πρώτοι και $\alpha \in \mathbb{Z}$. Δείξτε ότι $pq \mid \alpha^{pq} - \alpha^p - \alpha^q + \alpha$.
Απόδειξη: Παρατηρούμε ότι $\alpha^{pq} = (\alpha^p)^q \equiv \alpha^p \mod q$, από το «μικρό» θεώρημα του Fermat. Επομένως $q \mid \alpha^{pq} - \alpha^p$. Παρόμοια $\alpha^q \equiv \alpha \mod q \Leftrightarrow q \mid \alpha^q - \alpha$. Επομένως $q \mid \alpha^{pq} - \alpha^p - (\alpha^q - \alpha) = \alpha^{pq} - \alpha^p - \alpha^q + \alpha$. Με τον ίδιο τρόπο αποδεικνύουμε ότι $p \mid \alpha^{pq} - \alpha^p - \alpha^q + \alpha$. Επειδή οι πρώτοι p και q είναι διαφορετικοί, και το γινόμενό τους pq διαιρεί τον αριθμό $\alpha^{pq} - \alpha^p - \alpha^q + \alpha$. ■

Άσκηση 84. Βρείτε όλους τους θετικούς ακεραίους n, για τους οποίους ο αριθμός $(n-1)! + 1$ είναι δύναμη του n.
Λύση: Εφόσον $n^k = (n-1)! + 1$, έχουμε $n \mid (n-1)! + 1$. Από το Θεώρημα του Wilson έπεται ότι ο n είναι πρώτος. Άρα ο $n - 1$ είναι σύνθετος. Υποθέτουμε ότι $n \geq 7$. Τότε $n - 1 \geq 6 > 4$. Από την άσκηση 1.44 έχουμε ότι $n - 1 \mid (n-2)!$. Τώρα, $(n-1)! = n^k - 1 = (n-1)(n^{k-1} + n^{k-2} + \cdots + n + 1) \Leftrightarrow (n-2)! = n^{k-1} + n^{k-2} + \cdots + n + 1$. Εφόσον $n - 1 \mid (n-2)!$, θα έχουμε $\sum_{i=0}^{k-1} n^i \equiv 0 \mod (n-1)$. Αλλά $n^i \equiv 1 \mod (n-1)$, για κάθε $i = 0, 1, \ldots, k-1$. Επομένως $\sum_{i=0}^{k-1} n^i \equiv k \mod (n-1)$ και κατά συνέπεια $n - 1 \mid k$. Επομένως $k = \lambda(n-1)$, για κάποιον θετικό ακέραιο λ. Συνεπώς $(n-1)! = n^{\lambda(n-1)} - 1 \geq n^{n-1} - 1$. Αλλά $(n-1)! < n^{n-1} - 1$, για κάθε $n \geq 3$. Πράγματι, επαγωγικά για $n = 3$ έχουμε $(3-1)! = 2$ και $3^{3-1} - 1 = 8$.

Αν $(n-1)! < n^{n-1}-1$, τότε $n! < n^n - n < (n+1)^n - n < (n+1)^n - 1$. Συμπεραίνουμε λοιπόν ότι το $(n-1)!+1$ δεν είναι δύναμη του πρώτου n, αν $n \geq 7$. Τώρα, $(2-1)!+1 = 2 = 2^1$, $(3-1)!+1 = 3 = 3^1$ και $(5-1)!+1 = 24+1 = 25 = 5^2$. Άρα οι λύσεις του προβλήματος είναι οι πρώτοι αριθμοί 2, 3 και 5. ■

Άσκηση 85. Έστω p περιττός πρώτος. Δείξτε ότι αν η τετραγωνική ισοτιμία $x^2+1 \equiv 0 \mod p$ έχει λύση, τότε $p \equiv 1 \mod 4$.

Απόδειξη: Εφόσον p περιττός, ο $p-1$ είναι άρτιος και επομένως ο $\dfrac{p-1}{2}$ είναι θετικός ακέραιος.
Έστω α μια λύση της ισοτιμίας $x^2+1 \equiv 0 \mod p$, δηλαδή $\alpha^2 \equiv -1 \mod p$. Τότε $(\alpha, p) = 1$ και επομένως $\alpha^{p-1} \equiv 1 \mod p$. Αλλά, από τη σχέση $\alpha^2 \equiv -1 \mod p$ συνάγουμε ότι $\alpha^{p-1} = (\alpha^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \mod p$. Επομένως $1 \equiv (-1)^{\frac{p-1}{2}} \mod p \Leftrightarrow p \mid 1-(-1)^{\frac{p-1}{2}} = 0$ ή 2. Επειδή ο p είναι περιττός, έχουμε $(-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \dfrac{p-1}{2} \equiv 0 \mod 2 \Leftrightarrow p \equiv 1 \mod 4$. ■

Άσκηση 86. Έστω p περιττός πρώτος.
(i) Δείξτε ότι το σύνολο $\left\{-\dfrac{p-1}{2}, -\dfrac{p-3}{2}, \ldots, -1, 0, 1, 2, \ldots, \dfrac{p-3}{2}, \dfrac{p-1}{2}\right\}$ είναι ένα πλήρες σύστημα υπολοίπων modulo p και άρα ότι το σύνολο $\left\{, -\dfrac{p-1}{2}, -\dfrac{p-3}{2}, \ldots, -1, 1, \ldots, \dfrac{p-3}{2}, \dfrac{p-1}{2}\right\}$ είναι ένα πλήρες ανηγμένο σύστημα υπολοίπων modulo p.
(ii) Αν $q = \dfrac{p-1}{2}$, τότε δείξτε $(q!)^2 + (-1)^q \equiv 0 \mod p$. Συμπεράνατε ότι αν $p \equiv 1 \mod 4$, τότε το $q!$ είναι λύση της ισοτιμίας $x^2+1 \equiv 0 \mod p$ και αν $p \equiv 3 \mod 4$, τότε $q! \equiv \pm 1 \mod p$.
Απόδειξη: **(i)** Το σύνολο $\left\{0, 1, 2, \ldots, \dfrac{p-3}{2}, \dfrac{p-1}{2}, \dfrac{p+1}{2} = \dfrac{p-1}{2}+1, \ldots, p-1\right\}$ είναι ένα πλήρες σύστημα υπολοίπων modulo p. Τώρα, για κάθε $i = 1, 2, \ldots, \dfrac{p-1}{2}$ ο αριθμός $\dfrac{p-1}{2} + i = \dfrac{p+2i-1}{2}$ είναι ισοϋπόλοιπος modulo p με τον αριθμό $\dfrac{p+2i-1}{2} - p = -\dfrac{p-2i+1}{2}$. Για $i = 1, 2, \ldots, \dfrac{p-1}{2}$ παίρνουμε τους αριθμούς $-\dfrac{p-1}{2}, -\dfrac{p-3}{2}, \ldots, -1$.
(ii) Από το θεώρημα του Wilson έχουμε $(p-1)!+1 \equiv 0 \mod p$. Αλλά $(p-1)! = 1\cdot 2\cdot 3 \cdots \dfrac{p-1}{2} \cdot \dfrac{p+1}{2} \cdot \dfrac{p+3}{2} \cdots (p-1) \equiv 1\cdot 2\cdot 3 \cdots \dfrac{p-1}{2} \cdot \left(-\dfrac{p-1}{2}\right) \cdot \left(-\dfrac{p-3}{2}\right) \cdots (-3)\cdot(-2)\cdot(-1) = \left(1\cdot 2\cdot 3 \cdots \dfrac{p-1}{2}\right)^2 (-1)^{\frac{p-1}{2}} = (q!)^2(-1)^q$. Επομένως $(q!)^2(-1)^q + 1 \equiv 0 \mod p \Leftrightarrow (q!)^2 + (-1)^q \equiv 0 \mod p$.
Τώρα, αν $p \equiv 1 \mod 4 \Leftrightarrow 2 \,\Big|\, \dfrac{p-1}{2} = q$, τότε $(q!)^2 + 1 \equiv 0 \mod p$, δηλαδή το $q!$ είναι λύση της ισοτιμίας $x^2+1 \equiv 0 \mod p$. Τώρα, αν $p \equiv 3 \mod 4 \Leftrightarrow p-1 \equiv 2 \mod 4 \Leftrightarrow q = \dfrac{p-1}{2} \equiv 1 \mod 2$, θα έχουμε $(q!)^2 - 1 \equiv 0 \mod p \Leftrightarrow p \mid (q!)^2 - 1 = (q!-1)(q!+1) \Leftrightarrow \big(p \mid q!-1$ ή $p \mid q!+1\big) \Leftrightarrow \big(q! \equiv 1 \mod p$ ή $q! \equiv -1 \mod p\big)$. ■

Από τις δύο προηγούμενες ασκήσεις προκύπτει ότι αν p είναι περιττός πρώτος της μορφής $4k+1$, τότε δύο λύσεις της τετραγωνικής ισοτιμίας $x^2+1 \equiv 0 \mod p$ είναι οι $\left(\dfrac{p-1}{2}\right)!$ και $-\left(\dfrac{p-1}{2}\right)!$. Οι $\left(\dfrac{p-1}{2}\right)!$ και $-\left(\dfrac{p-1}{2}\right)!$ είναι ανισοϋπόλοιποι modulo p. Πράγματι, έστω $\left(\dfrac{p-1}{2}\right)! \equiv -\left(\dfrac{p-1}{2}\right)! \mod p$. Τότε $2 \cdot \left(\dfrac{p-1}{2}\right)! \equiv 0 \mod p$, που είναι άτοπο γιατί το 2 καθώς και όλοι οι ακέραιοι από το σύνολο $\left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$ είναι μικρότεροι του p και άρα πρώτοι προς αυτόν.

Άσκηση 87. Βρείτε δύο λύσεις των τετραγωνικών ισοτιμιών:
(i) $x^2 \equiv -1 \mod 29$ και **(ii)** $x^2 \equiv -1 \mod 37$.
Λύση: **(i)** Έχουμε $29 = 4\cdot 7 + 1$. Επομένως δύο λύσεις της $x^2 \equiv -1 \mod 29$ είναι οι $\pm\left(\dfrac{28}{2}\right)! = \pm 14!$.

Τώρα $14! = (2\cdot 14)(3\cdot 13)(4\cdot 12)(5\cdot 11)(6\cdot 10)(7\cdot 9)\cdot 8 = 28\cdot 39\cdot 48\cdot 55\cdot 60\cdot 63\cdot 8 \equiv -1\cdot 10(-10)(-3)\cdot 2\cdot 5\cdot 8 = = -100\cdot 3\cdot 80 \equiv -13\cdot 3\cdot 22 = -39\cdot 22 \equiv -10\cdot(-7) = 70 \equiv 12 \mod 29$. Μια άλλη λύση είναι η $-12 \equiv 17 \mod 29$.

(ii) Εφόσον $37 = 4\cdot 9 + 1$, εφαρμόζουμε την ίδια μέθοδο. Έχουμε $\left(\frac{36}{2}\right)! = 18!$. Έχουμε: $18! = = 2\cdot 18\cdot 3\cdot 17\cdot 4\cdot 16\cdot 5\cdot 15\cdot 6\cdot 14\cdot 7\cdot 13\cdot 8\cdot 12\cdot 9\cdot 11\cdot 10 = 36\cdot 51\cdot 64\cdot 75\cdot 84\cdot 91\cdot 96\cdot 99\cdot 10 \equiv -1\cdot 14(-10)\cdot 1\cdot 10\cdot 17\cdot 22\cdot 25\cdot 10 = = 100\cdot 14\cdot 17\cdot 22\cdot 25\cdot 10 \equiv 1000\cdot 14\cdot(-20)(-15)\cdot 25 \equiv 1\cdot 14\cdot 15\cdot 500 \equiv 210\cdot 19 \equiv 25\cdot 19 = 475 \equiv 31 \mod 37$. Μια άλλη λύση είναι η $-31 \equiv 6 \mod 37$. ■

Άσκηση 88. Έστω p περιττός πρώτος. Τότε

(i) $1^2\cdot 3^2\cdot 5^2\cdots(p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$ και **(ii)** $2^2\cdot 4^2\cdot 6^2\cdots(p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$.

Απόδειξη: (i) Έχουμε τις ακόλουθες σχέσεις:

$$\begin{cases} 1 \equiv 1-p = -(p-1) \mod p \\ 3 \equiv 3-p = -(p-3) \mod p \\ 5 \equiv 5-p = -(p-5) \mod p \\ \vdots \\ p-4 \equiv p-4-p = -4 \mod p \\ p-2 \equiv p-2-p = -2 \mod p \end{cases}$$

Πολλαπλασιάζουμε κατά μέλη και παίρνουμε: $1\cdot 3\cdot 5\cdots(p-2) \equiv (-1)^{\frac{p-1}{2}}\cdot 2\cdot 4\cdot 6\cdots(p-1) \mod p$. Αν πολλαπλασιάσουμε και τα δύο μέλη με $1\cdot 3\cdot 5\cdots(p-2)$ παίρνουμε

$$1^2\cdot 3^2\cdot 5^2\cdots(p-2)^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \underset{\substack{\text{θεώρημα}\\ \text{Wilson}}}{\equiv} (-1)^{\frac{p-1}{2}}(-1) = (-1)^{\frac{p+1}{2}} \mod p.$$

(ii) Αν υψώσουμε και τα δύο μέλη της σχέσης $(-1)^{\frac{p-1}{2}}\cdot 2\cdot 4\cdot 6\cdots(p-1) \equiv 1\cdot 3\cdot 5\cdots(p-2) \mod p$ στο τετράγωνο και με δεδομένο ότι $(-1)^{p-1} = 1$, αφού $p-1$ άρτιος, παίρνουμε $2^2\cdot 4^2\cdot 6^2\cdots(p-1)^2 \equiv \equiv 1^2\cdot 3^2\cdot 5^2\cdots(p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$. ■

Άσκηση 89. (Θεώρημα του Wolstenholme) Έστω $p \geq 5$ πρώτος αριθμός. Τότε $p^2 \mid \sum_{k=1}^{p-1} \frac{(p-1)!}{k}$.

Απόδειξη: Προφανώς $\sum_{k=1}^{p-1} \frac{(p-1)!}{k} = \sum_{k=1}^{p-1} \frac{(p-1)!}{p-k}$. Επομένως $2\cdot\sum_{k=1}^{p-1} \frac{(p-1)!}{k} = \sum_{k=1}^{p-1}\left(\frac{(p-1)!}{k} + \frac{(p-1)!}{p-k}\right) = = \sum_{k=1}^{p-1} \frac{p(p-1)!}{k(p-k)} = p\cdot\sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)}$. Επειδή $p \geq 5$, ο p είναι περιττός. Επομένως $k \neq p-k$, για κάθε $k = 1, 2, \ldots, p-1$. $\big($Σε αντίθετη περίπτωση $k = p-k \Leftrightarrow p = 2k$, άρτιος$\big)$. Άρα οι αριθμοί k και $p-k$ είναι διαφορετικοί παράγοντες του $(p-1)!$ και επομένως $\frac{(p-1)!}{k(p-k)} \in \mathbb{Z}$. Συνεπώς $\sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)} \in \mathbb{Z}$. Άρα $2\cdot\sum_{k=1}^{p-1} \frac{(p-1)!}{k} = p\cdot\sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)}$ είναι ακέραιο πολλαπλάσιο του p. Τώρα θα αποδείξουμε ότι

$$p \mid \sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)}.$$

Όπως στην απόδειξη του θεωρήματος του Wilson, για κάθε $k \in \{1, 2, \ldots, p-1\}$ υπάρχει μοναδικό $k' \in \{1, 2, \ldots, p-1\}$ τέτοιο, ώστε $kk' \equiv 1 \mod p$. Επίσης, καθώς το k διατρέχει όλους τους ακεραίους $1, 2, \ldots, p-1$ και το k' διατρέχει όλους τους ακεραίους $1, 2, \ldots, p-1$. Από τη σχέση $kk' \equiv 1 \mod p$ προκύπτει $k^2k'^2 \equiv 1 \mod p$. Επίσης $k(p-k) \equiv -k^2 \mod p \Rightarrow k(p-k)k'^2 \equiv -k^2k'^2 \equiv -1 \mod p \underset{((p-1)!,p)=1}{\Leftrightarrow} (p-1)!k(p-k)k'^2 \equiv -(p-1)! \mod p \underset{k(p-k)\mid(p-1)!}{\Leftrightarrow} \frac{(p-1)!}{k(p-k)} \equiv -(p-1)!k'^2 \underset{\substack{\text{θεώρημα}\\ \text{Wilson}}}{\equiv} k'^2$

$\mod p$, για κάθε $k = 1, 2, \ldots, p-1$. Άρα $\sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)} \equiv \sum_{k'=1}^{p-1} k'^2 = \frac{(p-1)p(2p-1)}{6} \mod p$. Επειδή $p \geq 5$, $(p, 6) = (p, 2 \cdot 3) = 1$. Άρα $p \mid (p-1)(2p-1)$ και επομένως $\frac{(p-1)p(2p-1)}{6} \equiv 0 \mod p$. Συνεπώς $p \Big| \sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)}$. Άρα $p^2 \Big| p \cdot \sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)} = 2 \cdot \sum_{k=1}^{p-1} \frac{(p-1)!}{k} \underset{(p,2)=1}{\Leftrightarrow} p^2 \Big| \sum_{k=1}^{p-1} \frac{(p-1)!}{k}$. ■

Άσκηση 90. Έστω $p \geq 5$ πρώτος αριθμός και $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p} = \frac{r}{ps}$. Τότε $p^3 \mid r - s$.

Απόδειξη: Έχουμε $p!s\Big(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}\Big) + (p-1)!s = (p-1)!r \Leftrightarrow ps \sum_{k=1}^{p-1} \frac{(p-1)!}{k} + (p-1)!s = $
$= (p-1)!r \Leftrightarrow ps \sum_{k=1}^{p-1} \frac{(p-1)!}{k} = (p-1)!(r-s)$. Από το θεώρημα του Wolstenholme έχουμε $p^2 \Big| \sum_{k=1}^{p-1} \frac{(p-1)!}{k}$. Επομένως $p^3 \mid (p-1)!(r-s) \underset{((p-1)!,p)=1}{\Leftrightarrow} p^3 \mid r - s$. ■

Άσκηση 91. Έστω n θετικός ακέραιος και p πρώτος με $p \leq n$. Τότε $\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \mod p$.

Επιπλέον, $p^k \Big| \binom{n}{p}$ αν και μόνον αν $p^k \Big| \left\lfloor \frac{n}{p} \right\rfloor$, για κάθε ακέραιο $k \geq 1$.

Απόδειξη: Υπενθυμίζουμε ότι το $\left\lfloor \frac{n}{p} \right\rfloor$ είναι το πηλίκο π της διαίρεσης $n : p$, δηλαδή $n = p\pi + \upsilon$, όπου $0 \leq \upsilon \leq p-1$. Οι p διαδοχικοί αριθμοί $n, n-1, n-2, \ldots, n-p+1$ αποτελούν πλήρες σύστημα υπολοίπων modulo n. Ο $p\pi$ είναι ένας από αυτούς γιατί $0 \leq \upsilon \leq p-1 \Leftrightarrow n-p+1 \leq p\pi = n-\upsilon \leq n$. Επομένως οι αριθμοί $n, n-1, \ldots, p\pi+1, p\pi-1 \ldots, n-p+1$ αποτελούν ένα πλήρες ανηγμένο σύστημα υπολοίπων modulo p. Άρα $n(n-1)\cdots(p\pi+1)(p\pi-1)\cdots(n-p+1) \equiv (p-1)! \mod p$. Επίσης
$\binom{n}{p} = \frac{n(n-1)\cdots(p\pi+1)p\pi(p\pi-1)\cdots(n-p+1)}{p!} = \frac{n(n-1)\cdots(p\pi+1)(p\pi-1)\cdots(n-p+1)}{(p-1)!} \cdot \pi$.

Επομένως $(p-1)!\binom{n}{p} = n(n-1)\cdots(p\pi+1)(p\pi-1)\cdots(n-p+1)\pi \equiv (p-1)!\pi \mod p \underset{((p-1)!,p)=1}{\Leftrightarrow}$
$\Leftrightarrow \binom{n}{p} \equiv \pi = \left\lfloor \frac{n}{p} \right\rfloor \mod p$.

Τώρα $p^k \Big| \binom{n}{p} \Leftrightarrow (p-1)!p^k \Big| (p-1)!\binom{n}{p} = n(n-1)\cdots(p\pi+1)(p\pi-1)\cdots(n-p+1)\pi$. Επειδή ο p είναι πρώτος προς το γινόμενο $n(n-1)\cdots(p\pi+1)(p\pi-1)\cdots(n-p+1)$, η τελευταία σχέση είναι ισοδύναμη με την $p^k \mid \pi = \left\lfloor \frac{n}{p} \right\rfloor$. ■

Άσκηση 92. Αν p πρώτος και $0 \leq k \leq p-1$, τότε δείξτε ότι $k!(p-1-k)! \equiv (-1)^{k+1} \mod p$.

Απόδειξη: Για $k = 0$ παίρνουμε $k!(p-1-k)! = 0! \cdot (p-1)! \equiv -1 = (-1)^{0+1} \mod p$ από το θεώρημα του Wilson. Για $k = p-1$ παίρνουμε $(p-1)! \cdot 0! \equiv -1 \mod p$. Έστω $p = 2$. Τότε $(-1)^{p-1+1} = (-1)^p = (-1)^2 = 1 \equiv -1 \mod 2$. Άρα, αν $p = 2$ και $k = 1$ η πρόταση ισχύει. Αν p περιττός, τότε $(-1)^{p-1+1} = (-1)^p = -1 \mod p$. Τελικώς συμπεραίνουμε ότι η πρόταση ισχύει για κάθε πρώτο p και $k = p-1$.
Έστω τώρα $p \geq 3$ και $0 < k < p-1$. Για κάθε $r = 1, \ldots, k$ έχουμε $r \equiv r - p = -(p-r) \mod p$. Επομένως $1 \cdot 2 \cdots k \equiv (-(p-1))(-(p-2)) \cdots (-(p-k)) \mod p \Leftrightarrow k! \equiv (-1)^k (p-k)(p-k+1) \cdots (p-2)(p-1) \mod p$. Επομένως $k!(p-1-k)! \equiv (-1)^k (p-1-k)!(p-k)(p-k+1)\cdots(p-2)(p-1) = (-1)^k (p-1)! \equiv (-1)^{k+1} \mod p$, από το θεώρημα του Wilson. ■

Άσκηση 93. Δείξτε ότι οι περιττοί πρώτοι διαιρέτες ενός αριθμού της μορφής $n^2 + 1$, όπου n θετικός ακέραιος, είναι της μορφής $4k + 1$.

Απόδειξη: Αν p περιττός πρώτος διαιρέτης του $n^2 + 1$, τότε $n^2 + 1 \equiv 0 \mod p$ και η τετραγωνική ισοτιμία $x^2 + 1$ έχει λύση. Το συμπέρασμα προκύπτει από την άσκηση 85. ■

2.5 Επίλυση γραμμικών ισοτιμιών

Πρόταση 2.37. Έστω n θετικός ακέραιος και $\alpha, \beta \in \mathbb{Z}$. Αν ο ακέραιος x επαληθεύει τη σχέση $\alpha x \equiv \beta \mod n$, τότε και κάθε ακέραιος x' με $x' \equiv x \mod n$ την επαληθεύει.
Απόδειξη: Έστω $\alpha x \equiv \beta \mod n$. Τότε έχουμε: $x' \equiv x \mod n \Rightarrow \alpha x' \equiv \alpha x \equiv \beta \mod n$. ■

Ορισμός 2.38. Μια σχέση της μορφής $\alpha x \equiv \beta \mod n$ λέγεται **γραμμική ισοτιμία**. Όπως προκύπτει από την προηγούμενη πρόταση, σε μια γραμμική ισοτιμία αναζητούμε **τις κλάσεις υπολοίπων modulo n**, των οποίων τα στοιχεία την επαληθεύουν. Ως λύση λοιπόν της γραμμικής ισοτιμίας $\alpha x \equiv \beta \mod n$ θεωρούμε όχι έναν απλό ακέραιο x, αλλά **ολόκληρη την κλάση** $\langle x \rangle$ modulo n στην οποία αυτός ανήκει.

Πρόταση 2.39. Έστω n θετικός ακέραιος και $\alpha, \beta \in \mathbb{Z}$. Αν $(\alpha, n) = 1$, τότε η γραμμική ισοτιμία $\alpha x \equiv \beta \mod n$ έχει **μοναδική λύση**, δηλαδή υπάρχει **μία μόνον κλάση** υπολοίπων modulo n της οποίας τα στοιχεία την επαληθεύουν.
Απόδειξη: Ύπαρξη: Εφόσον $(\alpha, n) = 1$, υπάρχουν $\kappa, \lambda \in \mathbb{Z}$ τέτοια, ώστε $\alpha\kappa + n\lambda = 1 \Leftrightarrow \alpha\kappa = 1 - \lambda n \Rightarrow$ $\Rightarrow \alpha(\kappa\beta) = \beta + (-\lambda\beta)n \Rightarrow \alpha(\kappa\beta) \equiv \beta \mod n$. Επομένως το $\kappa\beta$ (και όλα τα στοιχεία της κλάσης του) είναι λύση της ισοτιμίας.
Μοναδικότητα: Έστω $x, x' \in \mathbb{Z}$ με $\alpha x \equiv \beta \mod n$ και $\alpha x' \equiv \beta \mod n$. Αρκεί να δείξουμε ότι $x \equiv x' \mod n$. Πράγματι, από τις παραπάνω σχέσεις έχουμε $\alpha x \equiv \alpha x' \mod n \underset{\text{Λήμμα 2.21 (i)}}{\Leftrightarrow} x \equiv x' \mod n$. ■

Πόρισμα 2.40. Έστω n θετικός ακέραιος και $\alpha, \beta \in \mathbb{Z}$ με $(\alpha, n) = 1$. Η μοναδική λύση της ισοτιμίας $\alpha x \equiv \beta \mod n$ είναι η κλάση $\langle \alpha^{\varphi(n)-1}\beta \rangle$.
Απόδειξη: Από το θεώρημα του Euler έχουμε $\alpha^{\varphi(n)} \equiv 1 \mod n$. Επομένως $\alpha(\alpha^{\varphi(n)-1}\beta) \equiv \beta \mod n$. ■

Γενικότερα έχουμε το ακόλουθο θεώρημα:

Θεώρημα 2.41. Έστω n θετικός ακέραιος και $\alpha, \beta \in \mathbb{Z}$. Έστω $\delta = (\alpha, n)$. Τότε ισχύουν τα εξής:
(i) Η γραμμική ισοτιμία $\alpha x \equiv \beta \mod n$ έχει λύση αν και μόνον αν η γραμμική διοφαντική εξίσωση $\alpha x + ny = \beta$ έχει λύση.
(ii) Η γραμμική ισοτιμία $\alpha x \equiv \beta \mod n$ έχει λύση αν και μόνον αν $\delta \mid \beta$.
(iii) Αν $\langle x_0 \rangle$ είναι μια λύση της $\alpha x \equiv \beta \mod n$, τότε η γραμμική ισοτιμία έχει ακριβώς δ λύσεις. Αυτές είναι οι $\langle x_0 \rangle, \left\langle x_0 + \frac{n}{\delta} \right\rangle, \left\langle x_0 + 2 \cdot \frac{n}{\delta} \right\rangle, \ldots, \left\langle x_0 + (\delta - 1) \cdot \frac{n}{\delta} \right\rangle$.
Απόδειξη: (i) Έστω $x_0 \in \mathbb{Z}$ με $\alpha x_0 \equiv \beta \mod n \Leftrightarrow n \mid \alpha x_0 - \beta$. Αυτό είναι ισοδύναμο με το ότι υπάρχει $\lambda \in \mathbb{Z}$ τέτοιο, ώστε $\alpha x_0 - \beta = \lambda n \Leftrightarrow \alpha x_0 + (-\lambda)n = \beta$. Με άλλα λόγια, αν η $\alpha x \equiv \beta \mod n$ έχει λύση, τότε και η γραμμική διοφαντική εξίσωση $\alpha x + ny = \beta$ έχει λύση. Αντιστρόφως, υποθέτουμε ότι (x_0, y_0) είναι μια λύση της γραμμικής διοφαντικής εξίσωσης $\alpha x + ny = \beta$. Τότε $\alpha x_0 + ny_0 = \beta \Leftrightarrow \alpha x_0 = \beta - ny_0 \Rightarrow \alpha x_0 \equiv \beta \mod n$, δηλαδή η γραμμική ισοτιμία $\alpha x \equiv \beta \mod n$ έχει λύση.
(ii) Προκύπτει άμεσα από το προηγούμενο.
(iii) Έστω $\langle y \rangle$ μια λύση της $\alpha x \equiv \beta \mod n$. Εφόσον $\alpha x_0 \equiv \beta \mod n$, έχουμε $\alpha(y - x_0) \equiv 0 \mod n \Leftrightarrow$ $\Leftrightarrow n \mid \alpha(y - x_0) \Leftrightarrow \frac{n}{\delta} \mid \frac{\alpha}{\delta}(y - x_0) \underset{\left(\frac{n}{\delta}, \frac{\alpha}{\delta}\right)=1}{\Leftrightarrow} \frac{n}{\delta} \mid y - x_0 \Leftrightarrow y = x_0 + \lambda \cdot \frac{n}{\delta}$, όπου $\lambda \in \mathbb{Z}$.

Τώρα, προφανώς $\alpha\left(x_0 + \lambda \cdot \frac{n}{\delta}\right) = \alpha x_0 + \left(\lambda \cdot \frac{\alpha}{\delta}\right) \cdot n \equiv \alpha x_0 \equiv \beta \mod n$, για κάθε $\lambda \in \mathbb{Z}$. Τώρα θα πρέπει να διακρίνουμε τα $\lambda \in \mathbb{Z}$, τα οποία μας δίνουν όλες τις διαφορετικές κλάσεις υπολοίπων modulo n, οι οποίες είναι οι λύσεις της $\alpha x \equiv \beta \mod n$. Έχουμε: $x_0 + \lambda \cdot \frac{n}{\delta} \equiv x_0 + \lambda' \cdot \frac{n}{\delta} \mod n \Leftrightarrow n \mid (\lambda - \lambda') \cdot \frac{n}{\delta} \Leftrightarrow$ $\Leftrightarrow \delta n \mid n(\lambda - \lambda') \Leftrightarrow \delta \mid \lambda - \lambda' \Leftrightarrow \lambda \equiv \lambda' \mod \delta$. Άρα δύο ακέραιοι λ και λ' μας δίνουν την ίδια λύση modulo n, δηλαδή την ίδια κλάση modulo n, αν και μόνον αν ανήκουν στην ίδια κλάση υπολοίπων modulo δ. Επειδή το σύνολο $\{0, 1, 2, \ldots, \delta - 1\}$ αποτελεί πλήρες σύστημα υπολοίπων modulo δ, οι διαφορετικές λύσεις της $\alpha x \equiv \beta \mod n$ είναι ακριβώς οι δ κλάσεις με αντιπροσώπους $x_0, x_0 + \frac{n}{\delta}, x_0 + 2 \cdot \frac{n}{\delta}, \ldots, x_0 + (\delta - 1) \cdot \frac{n}{\delta}$. ■

Αντί να λέμε ότι οι $\langle x_0 \rangle, \left\langle x_0 + \frac{n}{\delta} \right\rangle, \left\langle x_0 + 2 \cdot \frac{n}{\delta} \right\rangle, \ldots, \left\langle x_0 + (\delta - 1) \cdot \frac{n}{\delta} \right\rangle$ είναι οι λύσεις της $\alpha x \equiv \beta$

$\bmod n$, πολλές φορές λέμε ότι οι $x_0, x_0 + \frac{n}{\delta}, x_0 + 2 \cdot \frac{n}{\delta}, \ldots, x_0 + (\delta - 1) \cdot \frac{n}{\delta} \mod n$ είναι οι λύσεις της ισοτιμίας αυτής.

Πρόταση 2.42. Έστω n θετικός ακέραιος και $\alpha, \beta \in \mathbb{Z}$ με $\delta = (\alpha, n) \mid \beta$. Τότε οι λύσεις της γραμμικής ισοτιμίας $\alpha x \equiv \beta \mod n$ δίνονται από τον τύπο

$$\frac{\alpha^{\varphi(n/\delta)-1}\beta}{\delta^{\varphi(n/\delta)}} + \lambda \cdot \frac{n}{\delta}, \text{ όπου } \lambda = 0, 1, \ldots, \delta - 1.$$

Απόδειξη: Ένας ακέραιος x_0 επαληθεύει τη σχέση $\alpha x \equiv \beta \mod n$ αν και μόνον αν $\alpha x_0 \equiv \beta \mod n \Leftrightarrow$ $\Leftrightarrow \frac{\alpha}{\delta} x_0 \equiv \frac{\beta}{\delta} \mod \frac{n}{\delta}$. Επειδή $\left(\frac{\alpha}{\delta}, \frac{n}{\delta}\right) = 1$, σύμφωνα με το πόρισμα 2.33, ως x_0 μπορούμε να πάρουμε τον ακέραιο $\left(\frac{\alpha}{\delta}\right)^{\varphi(n/\delta)-1} \cdot \frac{\beta}{\delta} = \frac{\alpha^{\varphi(n/\delta)-1}\beta}{\delta^{\varphi(n/\delta)}}$. ■

Άσκηση 94. Να λύσετε τις παρακάτω γραμμικές ισοτιμίες:
(i) $7x \equiv 3 \mod 11$.
(ii) $42x \equiv 63 \mod 105$.
(iii) Να λύσετε τη γραμμική ισοτιμία $20x \equiv 10 \mod 15$.
Λύση: (i) Λύνουμε τη γραμμική εξίσωση $7x - 11y = 3$. Εφαρμόζοντας τον ευκλείδειο αλγόριθμο, βρίσκουμε $11 \cdot 2 - 7 \cdot 3 = 1 \Leftrightarrow 7(-9) + 11 \cdot 6 = 3$. Επομένως $7(-9) \equiv 3 \mod 11$, δηλαδή το $-9 \equiv 2 \mod 11$ είναι λύση της ισοτιμίας. Επειδή $(7, 11) = 1$, η λύση $2 \mod 11$ είναι και η μοναδική.
(ii) Έχουμε $(42, 105) = (2 \cdot 3 \cdot 7, 3 \cdot 5 \cdot 7) = 3 \cdot 7 = 21 \mid 63$. Άρα η ισοτιμία έχει λύση. Επειδή $(42, 105) = 21$, η ισοτιμία $42x \equiv 63 \mod 105$ έχει ακριβώς 21 λύσεις modulo 105. Αρκεί να βρούμε μία. Λύνουμε τη γραμμική εξίσωση $42x - 105y = 63$. Κατά τα γνωστά μια λύση της είναι η $(x, y) = (-6, -3)$. Άρα μία λύση της ισοτιμίας είναι η $-6 \equiv 99 \mod 105$. Επειδή $\frac{105}{21} = 5$, όλες οι λύσεις είναι της μορφής $99 + 5\lambda$ modulo 105, όπου $\lambda = 0, 1, 2, \ldots, 20$. Αυτές είναι: $\boxed{99}, 99 + 5 = \boxed{104}, 104 + 5 \equiv \boxed{4}, 4 + 5 =$ $= \boxed{9}, 9 + 5 = \boxed{14}, 14 + 5 = \boxed{19}, 19 + 5 = \boxed{24}, 24 + 5 = \boxed{29}, 29 + 5 = \boxed{34}, 34 + 5 = \boxed{39}, 39 + 5 =$ $= \boxed{44}, 44 + 5 = \boxed{49}, 49 + 5 = \boxed{54}, 54 + 5 = \boxed{59}, 59 + 5 = \boxed{64}, 64 + 5 = \boxed{69}, 69 + 5 = \boxed{74}, 74 + 5 =$ $= \boxed{79}, 79 + 5 = \boxed{84}, 84 + 5 = \boxed{89}, 89 + 5 = \boxed{94}$ modulo 105.
(iii) Προφανώς $(20, 15) = 5 \mid 10$. Η γραμμική ισοτιμία $20x \equiv 5 \mod 15$ αντιστοιχεί στην εξίσωση $20x + 15y = 10$. Μια λύση αυτής είναι η $(2, -2)$. Επίσης $\frac{15}{5} = 3$. Οι λύσεις λοιπόν της γραμμικής ισοτιμίας είναι $\boxed{2} \mod 15$, $2 + 3 \equiv \boxed{5} \mod 15$, $2 + 2 \cdot 3 \equiv \boxed{8} \mod 15$, $2 + 3 \cdot 3 \equiv \boxed{11} \mod 15$ και $2 + 4 \cdot 3 \equiv \boxed{14} \mod 15$. ■

2.6 Το Κινεζικό Θεώρημα υπολοίπων

Στη συνέχεια θα ασχοληθούμε με συστήματα γραμμικών ισοτιμιών. Συγκεκριμένα θα αποδείξουμε το λεγόμενο **Κινεζικό Θεώρημα υπολοίπων**:

Θεώρημα 2.43. (Κινεζικό Θεώρημα υπολοίπων) Υποθέτουμε ότι οι θετικοί ακέραιοι $n_1, n_2, \ldots, n_k$ είναι ανά δύο πρώτοι μεταξύ τους, δηλαδή $(n_i, n_j) = 1$ αν $i \neq j$.
Έστω $\beta_1, \beta_2, \ldots, \beta_k$ τυχόντες ακέραιοι. Τότε το ακόλουθο σύστημα γραμμικών ισοτιμιών

$$\begin{cases} x \equiv \beta_1 \mod n_1 \\ x \equiv \beta_2 \mod n_2 \\ \quad \vdots \\ x \equiv \beta_k \mod n_k \end{cases} \qquad (1)$$

έχει μοναδική λύση modulo $(n_1 n_2 \cdots n_k)$.
Απόδειξη: Θέτουμε $\mathrm{M}_i = \frac{n_1 n_2 \cdots n_k}{n_i} = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$, για κάθε $i = 1, 2, \ldots, k$. Εφόσον $(n_i, n_j) =$ $= 1$, για κάθε $j \neq i$, έχουμε $(\mathrm{M}_i, n_i) = 1$. Επομένως η γραμμική ισοτιμία $\mathrm{M}_i x \equiv \beta_i \mod n_i$ έχει μοναδική

λύση x_i modulo n_i. Θέτουμε $x = \mathrm{M}_1x_1 + \mathrm{M}_2x_2 + \cdots + \mathrm{M}_kx_k$.
Έστω $i \in \{1, 2, \ldots, k\}$. Επειδή $n_i \mid \mathrm{M}_j = n_1 \cdots n_{j-1}n_{j+1} \cdots n_k$, για κάθε $j \neq i$, θα έχουμε $\mathrm{M}_jx_j \equiv 0 \mod n_i$. Επομένως $x = \mathrm{M}_1x_1 + \mathrm{M}_2x_2 + \cdots + \mathrm{M}_kx_k \equiv \mathrm{M}_ix_i \equiv \beta_i \mod n_i$, για κάθε $i = 1, 2, \ldots, k$.
Έστω y μια άλλη λύση του συστήματος (1), δηλαδή $y \equiv \beta_i \mod n_i$, για κάθε $i = 1, 2, \ldots, k$. Τότε $x \equiv y \mod n_i \Leftrightarrow n_i \mid x - y$, για κάθε $i = 1, 2, \ldots, k$. Εφόσον τα n_i είναι ανά δύο πρώτα μεταξύ τους, από το (iii) της πρότασης 1.21 (σελ. 20) προκύπτει ότι $n_1n_2 \cdots n_k \mid x - y \Leftrightarrow x \equiv y \mod (n_1n_2 \cdots n_k)$. ■

Θα αποδείξουμε τώρα μια γενίκευση του Κινεζικού Θεωρήματος.

Θεώρημα 2.44. Υποθέτουμε ότι οι θετικοί ακέραιοι $n_1, n_2, \ldots, n_k$ είναι ανά δύο πρώτοι μεταξύ τους, δηλαδή $(n_i, n_j) = 1$ αν $i \neq j$ και $(\alpha_i, n_i) = 1$, για κάθε $i = 1, 2, \ldots, k$.
Έστω $\beta_1, \beta_2, \ldots, \beta_k$ τυχόντες ακέραιοι. Τότε το ακόλουθο σύστημα γραμμικών ισοτιμιών

$$\begin{cases} \alpha_1x \equiv \beta_1 \mod n_1 \\ \alpha_2x \equiv \beta_2 \mod n_2 \\ \quad \vdots \\ \alpha_kx \equiv \beta_k \mod n_k \end{cases} \qquad \textbf{(2)}$$

έχει μοναδική λύση modulo $(n_1n_2 \cdots n_k)$.
Απόδειξη: Εφόσον $(\alpha_i, n_i) = 1$, η γραμμική ισοτιμία $\alpha_ix \equiv 1 \mod n_i$ έχει μοναδική λύση α_i' modulo n_i, για κάθε $i = 1, 2, \ldots, k$. Το σύστημα των ισοτιμιών γίνεται

$$\begin{cases} x \equiv \alpha_1'\beta_1 \mod n_1 \\ x \equiv \alpha_2'\beta_2 \mod n_2 \\ \quad \vdots \\ x \equiv \alpha_k'\beta_k \mod n_k \end{cases} \qquad \textbf{(2')}$$

το οποίο επιλύεται όπως προηγουμένως. ■

Άσκηση 95. Να λύσετε το σύστημα

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 4 \\ x \equiv 5 \mod 7 \end{cases}$$

των γραμμικών ισοτιμιών modulo $84 = 2^2 \cdot 3 \cdot 7$.
Λύση: Λύνουμε την ισοτιμία $4 \cdot 7x = 28x \equiv 1 \mod 3$, δηλαδή τη γραμμική εξίσωση $28x + 3y = 1$. Έχουμε $28 = 3 \cdot 9 + 1 \Leftrightarrow 28 \cdot 1 + 3(-9) = 1$. Μια λύση της ισοτιμίας $28x \equiv 1 \mod 3$ είναι η $1 \mod 3$.
Ακολούθως λύνουμε την $3 \cdot 7x = 21x \equiv 2 \mod 4$. Έχουμε $21x + 4y = 2$, $21 = 4 \cdot 5 + 1 \Leftrightarrow 21 \cdot 1 + 4(-5) = 1 \Leftrightarrow 21 \cdot 2 + 4(-10) = 2$. Άρα μια λύση της ισοτιμίας $21x \equiv 2 \mod 4$ είναι η $2 \mod 4$.
Τέλος, λύνουμε την $3 \cdot 4x = 12x \equiv 5 \mod 7$. Έχουμε $12x + 7y = 5$, $12 = 7 + 5 \Leftrightarrow 12 \cdot 1 + 7(-1) = 5$. Άρα μια λύση της ισοτιμίας $12x \equiv 5 \mod 7$ είναι η $1 \mod 7$.
Θεωρούμε τον αριθμό $x = 28 \cdot 1 + 21 \cdot 2 + 12 \cdot 1 = 28 + 42 + 12 = 82$. Η κλάση $82 \mod 84$ είναι η μοναδική λύση του συστήματος. ■

Άσκηση 96. Να λύσετε το σύστημα

$$\begin{cases} 6x \equiv 3 \mod 9 \\ 3x \equiv 5 \mod 4 \\ 7x \equiv 1 \mod 5 \end{cases}$$

των γραμμικών ισοτιμιών modulo $180 = 9 \cdot 4 \cdot 5$.
Λύση: Λύνουμε τη γραμμική ισοτιμία $6x \equiv 3 \mod 9$, η οποία έχει λύση αφού $(6, 9) = 3 \mid 3$. Έχουμε $9 = 6 + 3 \Leftrightarrow 6(-1) + 9 \cdot 1 = 3$. Επειδή $\dfrac{9}{(6,3)} = 3$, η γραμμική ισοτιμία $6x \equiv 3 \mod 9$ έχει τρεις ανισοϋπόλοιπες λύσεις modulo 9. Αυτές είναι: $-1 \equiv 8 \mod 9$, $-1 + 3 = 2 \mod 9$ και $-1 + 2 \cdot 3 = 5 \mod 9$. Εφόσον $(3, 4) = 1$ και $(7, 5) = 1$, οι άλλες δύο ισοτιμίες έχουν μοναδική λύση.

Για τη δεύτερη έχουμε: $3(-1)+4\cdot 1=1 \Leftrightarrow 3(-5)+4\cdot 5=5$. Η μοναδική λύση της δεύτερης ισοτιμίας είναι η $-5\equiv 3 \mod 4$.
Για την τρίτη έχουμε: $7=5+2$, $5=2\cdot 2+1$. Επομένως $1=5-2\cdot 2=5-2(7-5)=7(-2)+5\cdot 3$. Η μοναδική λύση της ισοτιμίας $7x\equiv 1 \mod 5$ είναι η $-2\equiv 3 \mod 5$. Επειδή η πρώτη ισοτιμία έχει τρεις λύσεις, το σύστημα σπάει σε τρία συστήματα, τα ακόλουθα:

$$\begin{cases} x\equiv 8 \mod 9 \\ x\equiv 3 \mod 4 \\ x\equiv 3 \mod 5 \end{cases} \quad (1) \qquad \begin{cases} x\equiv 2 \mod 9 \\ x\equiv 3 \mod 4 \\ x\equiv 3 \mod 5 \end{cases} \quad (2) \qquad \begin{cases} x\equiv 5 \mod 9 \\ x\equiv 3 \mod 4 \\ x\equiv 3 \mod 5 \end{cases} \quad (3)$$

Για το σύστημα (1) λύνουμε την πρώτη ισοτιμία $4\cdot 5x\equiv 8 \mod 9 \Leftrightarrow 20x\equiv 8 \mod 9$. Έχουμε $20+9(-2)=2 \Leftrightarrow 20\cdot 4+9(-8)=8 \Rightarrow \boxed{20\cdot 4\equiv 8 \mod 9}$. Για τη δεύτερη έχουμε $20x\equiv 2 \mod 9$. Άρα $20x-9y=3$. Έχουμε $45\cdot 1+4(-11)=1 \Leftrightarrow 45\cdot 3+4(-33)=3 \Rightarrow \boxed{45\cdot 3\equiv 3 \mod 4}$.
Για την τρίτη, $36x\equiv 3 \mod 5$. Αλλά $36\cdot 1+5(-7)=1 \Leftrightarrow 36\cdot 3+5(-21)=3 \Rightarrow \boxed{36\cdot 3\equiv 3 \mod 5}$.
Παίρνουμε ως λύση modulo 180 την κλάση $20\cdot 4+45\cdot 3+36\cdot 3=323\equiv \boxed{143 \mod 180}$.
Στα υπόλοιπα συστήματα το μόνο που αλλάζει είναι η πρώτη ισοτιμία. Για το δεύτερο έχουμε $20\cdot 1+9(-2)=2 \Rightarrow 20\cdot 1\equiv 2 \mod 9$.
Παίρνουμε ως λύση του συστήματος την κλάση $20\cdot 1+45\cdot 3+36\cdot 3=263\equiv \boxed{83 \mod 180}$.
Για το τρίτο έχουμε $20\cdot(-2)+9\cdot 5=5 \Rightarrow 20(-2)\equiv 5 \mod 9$.
Παίρνουμε ως λύση του συστήματος την κλάση $20\cdot(-2)+45\cdot 3+36\cdot 3=203\equiv \boxed{23 \mod 180}$.

Άσκηση 97. Να λύσετε το σύστημα

$$\begin{cases} 3x\equiv 2 \mod 5 \\ -2x\equiv 2 \mod 3 \\ 5x\equiv 9 \mod 11 \\ 7x\equiv 11 \mod 13 \end{cases}$$

των γραμμικών ισοτιμιών modulo $5\cdot 3\cdot 11\cdot 13=2145$.
Λύση: Λύνουμε πρώτα την ισοτιμία $3x\equiv 2 \mod 5$. Έχουμε $3x-5y=2$ η αντίστοιχη γραμμική εξίσωση. $5=3+2$, $3=2+1$, $1=3-2=3-(5-3)=3\cdot 2-5$. Άρα $3\cdot 4-5\cdot 2=2 \Rightarrow 3\cdot 4\equiv 2 \mod 5$. Επειδή $(3,5)=1$, άλλη λύση modulo 5 δεν υπάρχει. Άρα $x\equiv 4 \mod 5$.
Η δεύτερη ισοτιμία έχει την προφανή και μοναδική (εφόσον $(-2,3)=1$) λύση $x\equiv -1\equiv 2 \mod 3$.
Για τους ίδιους λόγους και η κάθε μια από τις υπόλοιπες δύο ισοτιμίες έχει μοναδική λύση. Επειδή οι αριθμοί 11 και 13 είναι σχετικώς μικροί, μπορούμε και μέσω δοκιμών να βρούμε αυτές τις λύσεις. Έχουμε λοιπόν: $3\cdot 5=15\equiv 4 \mod 11$, $4\cdot 5=20\equiv 9 \mod 11$. Άρα $x\equiv 4 \mod 11$. Αλλά για τη δεύτερη (ύστερα από δικές μου δοκιμές) προσφέρεται η μέθοδος της γραμμικής εξίσωσης. Έχουμε: $7x-13y=11$. Με τον ευκλείδειο αλγόριθμο έχουμε: $13=7+6$, $7=6+1$. Άρα $1=7-6=7-(13-7)=7\cdot 2-13$. Επομένως $7\cdot 22-13\cdot 11=11 \Rightarrow 7\cdot 22\equiv 11 \mod 13 \Leftrightarrow 7\cdot 9\equiv 11 \mod 13$. Άρα $x\equiv 9 \mod 13$. Οδηγούμαστε λοιπόν στο σύστημα:

$$\begin{cases} x\equiv 4 \mod 5 \\ x\equiv 2 \mod 3 \\ x\equiv 4 \mod 11 \\ x\equiv 9 \mod 13 \end{cases}$$

Έχουμε την πρώτη ισοτιμία: $3\cdot 11\cdot 13x\equiv 4 \mod 5 \Leftrightarrow 429x\equiv 4 \mod 5 \Leftrightarrow 4x\equiv 4 \mod 5 \Leftrightarrow x\equiv 1 \mod 5$.
Για τη δεύτερη: $5\cdot 11\cdot 13x\equiv 2 \mod 3 \Leftrightarrow 2\cdot 2\cdot 1x\equiv 2 \mod 3 \Leftrightarrow 4x\equiv 2 \mod 3 \Leftrightarrow x\equiv 2 \mod 3$.
Για την τρίτη: $5\cdot 3\cdot 13x\equiv 4 \mod 11 \Leftrightarrow 15\cdot 13x\equiv 4 \mod 11 \Leftrightarrow 4\cdot 2x\equiv 4 \mod 11 \Leftrightarrow 2x\equiv 1\equiv 12 \mod 11 \Leftrightarrow x\equiv 6 \mod 11$.
Για την τέταρτη: $5\cdot 3\cdot 11x\equiv 9 \mod 13 \Leftrightarrow 15\cdot 11x\equiv 9 \mod 13 \Leftrightarrow 2\cdot 11x\equiv 9 \mod 13 \Leftrightarrow 22x\equiv 9 \mod 13 \Leftrightarrow 9x\equiv 9 \mod 13 \Leftrightarrow x\equiv 1 \mod 13$. Ο ζητούμενος αριθμός modulo $5\cdot 3\cdot 11\cdot 13=2145$ είναι ο $3\cdot 11\cdot 13\cdot 1+5\cdot 11\cdot 13\cdot 2+5\cdot 3\cdot 13\cdot 6+5\cdot 3\cdot 11\cdot 1=429+1430+1170+165=3194\equiv 1049 \mod 2145$. ■

Άσκηση 98. Ποιο είναι το υπόλοιπο της διαίρεσης του 1234567^{7777} δια του 364;
Λύση: Παρατηρούμε ότι $364 = 4 \cdot 7 \cdot 13$. Επίσης $1234567 = 308641 \cdot 4 + 3 \Leftrightarrow 1234567 \equiv 3 \mod 4$. Ακόμη $\varphi(4) = 2$. Επομένως $1234567 \equiv 3 \mod 4 \Rightarrow 1234567^{7777} \equiv 3^{7777} = 3^{2 \cdot 3888+1} = (3^2)^{3888} \cdot 3 \equiv 3 \mod 4$.
Επίσης, $1234567 = 176366 \cdot 7 + 5$ και $\varphi(7) = 6$. Επομένως $1234567 \equiv 5 \mod 7 \Rightarrow 1234567^{7777} \equiv 5^{7777} = = 5^{6 \cdot 1296+1} = (5^6)^{1296} \cdot 5 \equiv 5 \mod 7$.
Επίσης, $1234567 = 94966 \cdot 13 + 9$ και $\varphi(13) = 12$. Επομένως $1234567 \equiv 9 \mod 13 \Rightarrow 1234567^{7777} \equiv 9^{7777} = = 9^{12 \cdot 648+1} = (9^{12})^{648} \cdot 9 \equiv 9 \mod 13$. Λύνουμε τώρα το ακόλουθο σύστημα γραμμικών ισοτιμιών:

$$\begin{cases} x \equiv 3 \mod 4 \\ x \equiv 5 \mod 7 \\ x \equiv 9 \mod 13 \end{cases}$$

Πρώτα λύνουμε την ισοτιμία $7 \cdot 13x \equiv 3 \mod 4 \Leftrightarrow (-1) \cdot 1 \cdot x \equiv 3 \mod 4 \Leftrightarrow x \equiv -3 \equiv \boxed{1} \mod 4$.
Ακολούθως την ισοτιμία $4 \cdot 13x \equiv 5 \mod 7 \Leftrightarrow -4x \equiv 5 \mod 7 \Leftrightarrow 4x \equiv -5 \equiv 2 \mod 7 \Leftrightarrow 8x \equiv 4 \mod 7 \Leftrightarrow x \equiv \boxed{4} \mod 7$.
Τέλος, λύνουμε την ισοτιμία $4 \cdot 7x \equiv 9 \mod 13 \Leftrightarrow 28x \equiv 9 \mod 13 \Leftrightarrow 2x \equiv 9 \mod 13 \Leftrightarrow 14x \equiv 7 \cdot 9 = 63 \equiv 11 \mod 13 \Leftrightarrow x \equiv \boxed{11} \mod 13$.
Λύση του συστήματος modulo $4 \cdot 7 \cdot 13 = 364$ είναι η $7 \cdot 13 \cdot 1 + 4 \cdot 13 \cdot 4 + 4 \cdot 7 \cdot 11 = 607 \equiv 243 \mod 364$. ■

2.7 Ο δακτύλιος $\mathbb{Z}_n$, όπου $n > 1$

Σύμφωνα με την προηγούμενη παράγραφο, στην οποία ενδιαφερόμαστε για τις κλάσεις ισοδυναμίας modulo n ως λύσεις των γραμμικών ισοτιμιών, αλλά και με βάση την πρόταση 2.11 το ενδιαφέρον αρχίζει να επικεντρώνεται περισσότερο στις κλάσεις ισοδυναμίας παρά στους απλούς ακεραίους.

Συμβολισμός: Έστω n θετικός ακέραιος, μεγαλύτερος της μονάδας. Συμβολίζουμε με $\mathbb{Z}_n$ το σύνολο όλων των κλάσεων ισοδυναμίας (ή υπολοίπων) modulo n. Έτσι, $\mathbb{Z}_n = \{\langle 0\rangle, \langle 1\rangle, \langle 2\rangle, \ldots, \langle n-1\rangle\}$. Θα μπορούσαμε φυσικά να επιλέξουμε άλλους αντιπροσώπους για τις κλάσεις modulo n. Για παράδειγμα, $\langle 0\rangle = \langle n\rangle = \langle -2n\rangle$ ή $\langle n-1\rangle = \langle -1\rangle$, αφού $n \equiv -2n \equiv 0 \mod n$ και $n - 1 \equiv -1 \mod n$.

Στο σύνολο $\mathbb{Z}_n$ ορίζουμε δύο (εσωτερικές) πράξεις: Την **πρόσθεση** $+$ και τον **πολλαπλασιασμό** $\cdot$ ως εξής: $\langle x\rangle + \langle y\rangle = \langle x+y\rangle$ και $\langle x\rangle \cdot \langle y\rangle = \langle xy\rangle$.

Υπάρχει όμως ένα πρόβλημα. Οι πράξεις αυτές ορίστηκαν μέσω **κάποιων συγκεκριμένων αντιπροσώπων** των κλάσεων ισοδυναμίας modulo n. Τι θα γίνει αν αλλάξουμε τους αντιπροσώπους των κλάσεων; Τα αποτελέσματα της πρόσθεσης και του πολλαπλασιασμού θα παραμείνουν τα ίδια; Τέτοια προβλήματα στα μαθηματικά εμφανίζονται συχνά και έχουν να κάνουν με το αν οι πράξεις εν προκειμένω είναι «**καλά ορισμένες**». Εδώ τα πράγματα είναι εύκολα: Έστω $\langle x\rangle = \langle x'\rangle$ και $\langle y\rangle = \langle y'\rangle$. Θα πρέπει να αποδείξουμε ότι $\langle x+y\rangle = \langle x'+y'\rangle$ και $\langle xy\rangle = \langle x'y'\rangle$, δηλαδή τα αποτελέσματα (κλάσεις modulo n) των πράξεων είναι ανεξάρτητα απ' τους αντιπροσώπους των κλάσεων που χρησιμοποιήσαμε.
Πράγματι, οι σχέσεις $\langle x\rangle = \langle x'\rangle$ και $\langle y\rangle = \langle y'\rangle$ γράφονται ισοδύναμα $x \equiv x' \mod n$ και $y \equiv y' \mod n$. Από την πρόταση 2.11 προκύπτει ότι $x + y \equiv x' + y' \mod n$ και $xy \equiv x'y' \mod n$. Οι τελευταίες σχέσεις είναι ισοδύναμες με τις $\langle x+y\rangle = \langle x'+y'\rangle$ και $\langle xy\rangle = \langle x'y'\rangle$ αντίστοιχα.
Συμπέρασμα: Η πρόσθεση και ο πολλαπλασιασμός των κλάσεων ισοδυναμίας modulo n, όπως αυτές ορίστηκαν **είναι ανεξάρτητες από τους αντιπροσώπους των κλάσεων αυτών**. Όποιους αντιπροσώπους και να χρησιμοποιήσουμε το αποτέλεσμα δεν αλλάζει.

Θεώρημα 2.45. Το σύνολο $\mathbb{Z}_n$ εφοδιασμένο με τις ανωτέρω πράξεις της πρόσθεσης και του πολλαπλασιασμού είναι ένας **μη τετριμμένος μεταθετικός δακτύλιος με μονάδα**. (Βλέπε ορισμό Β'.12 του παραρτήματος Β'). Συγκεκριμένα ισχύουν τα εξής:
α) Το ζεύγος $(\mathbb{Z}_n, +)$ είναι αβελιανή ομάδα. Δηλαδή:
(i) $\langle x\rangle + \langle y\rangle = \langle y\rangle + \langle x\rangle$, για κάθε $\langle x\rangle, \langle y\rangle \in \mathbb{Z}_n$.

(ii) $\langle x\rangle + (\langle y\rangle + \langle z\rangle) = (\langle x\rangle + \langle y\rangle) + \langle z\rangle$, για κάθε $\langle x\rangle, \langle y\rangle, \langle z\rangle \in \mathbb{Z}_n$.
(iii) Υπάρχει ουδέτερο στοιχείο για την πρόσθεση, το οποίο είναι η κλάση $\langle 0\rangle$, με $\langle x\rangle + \langle 0\rangle \big(= \langle 0\rangle + \langle x\rangle \big) = \langle x\rangle$, για κάθε $\langle x\rangle \in \mathbb{Z}_n$.
(iv) Για κάθε $\langle x\rangle \in \mathbb{Z}_n$ υπάρχει (μοναδικό) στοιχείο $-\langle x\rangle$ τέτοιο, ώστε $\langle x\rangle + (-\langle x\rangle) = \big((-\langle x\rangle) + \langle x\rangle\big) = \langle 0\rangle$.

β) Το ζεύγος $(\mathbb{Z}_n, \cdot)$ είναι ημιομάδα, δηλαδή ο πολλαπλασιασμός είναι προσεταιριστικός, δηλαδή
(v) $\langle x\rangle(\langle y\rangle\langle z\rangle) = (\langle x\rangle\langle y\rangle)\langle z\rangle$, για κάθε $\langle x\rangle, \langle y\rangle, \langle z\rangle \in \mathbb{Z}_n$.

γ) **(vi)** Ο πολλαπλασιασμός είναι μεταθετικός, δηλαδή $\langle x\rangle \cdot \langle y\rangle = \langle y\rangle \cdot \langle x\rangle$, για κάθε $\langle x\rangle, \langle y\rangle \in \mathbb{Z}_n$.
(vii) Υπάρχει ουδέτερο στοιχείο για τον πολλαπλασιασμό, το οποίο είναι η κλάση $\langle 1\rangle$, με $\langle x\rangle \cdot \langle 1\rangle = \big(= \langle 1\rangle \cdot \langle x\rangle\big) = \langle x\rangle$, για κάθε $\langle x\rangle \in \mathbb{Z}_n$.

δ) Ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση, δηλαδή
(viii) $\langle x\rangle(\langle y\rangle + \langle z\rangle) = \langle x\rangle\langle y\rangle + \langle x\rangle\langle z\rangle$, για κάθε $\langle x\rangle, \langle y\rangle, \langle z\rangle \in \mathbb{Z}_n$. (Λόγω της μεταθετικότητας του πολλαπλασιασμού έχουμε $(\langle x\rangle + \langle y\rangle)\langle z\rangle = \langle z\rangle(\langle x\rangle + \langle y\rangle) = \langle z\rangle\langle x\rangle + \langle z\rangle\langle y\rangle = \langle x\rangle\langle z\rangle + \langle y\rangle\langle z\rangle$, για κάθε $\langle x\rangle, \langle y\rangle, \langle z\rangle \in \mathbb{Z}_n$).

Απόδειξη: **(i)** $\langle x\rangle + \langle y\rangle = \langle x + y\rangle = \langle y + x\rangle = \langle y\rangle + \langle x\rangle$.
(ii) $\langle x\rangle + (\langle y\rangle + \langle z\rangle) = \langle x\rangle + \langle y + z\rangle = \langle x + (y + z)\rangle = \langle (x + y) + z\rangle = \langle x + y\rangle + \langle z\rangle = (\langle x\rangle + \langle y\rangle) + \langle z\rangle$.
(iii) $\langle x\rangle + \langle 0\rangle = \langle x + 0\rangle = \langle x\rangle$.
(iv) Το $-\langle x\rangle$ είναι το $\langle -x\rangle = \langle n - x\rangle$. Πράγματι, $\langle x\rangle + \langle -x\rangle = \langle x + (-x)\rangle = \langle 0\rangle$.
(v) $\langle x\rangle(\langle y\rangle\langle z\rangle) = \langle x\rangle\langle yz\rangle = \langle x(yz)\rangle = \langle (xy)z\rangle = \langle xy\rangle\langle z\rangle = (\langle x\rangle\langle y\rangle)\langle z\rangle$.
(vi) $\langle x\rangle\langle y\rangle = \langle xy\rangle = \langle yx\rangle = \langle y\rangle\langle x\rangle$.
(vii) $\langle x\rangle\langle 1\rangle = \langle x \cdot 1\rangle = \langle x\rangle$.
(viii) $\langle x\rangle(\langle y\rangle + \langle z\rangle) = \langle x\rangle\langle y + z\rangle = \langle x(y + z)\rangle = \langle xy + xz\rangle = \langle xy\rangle + \langle xz\rangle = \langle x\rangle\langle y\rangle + \langle x\rangle\langle z\rangle$. ■

Με βάση τα παραπάνω, μπορούμε να ορίσουμε δυνάμεις κλάσεων ισοδυναμίας βάσει του τύπου $\langle x\rangle^k = \langle x^k\rangle$, όπου k θετικός ακέραιος. Για μια πιο ολοκληρωμένη εικόνα ο αναγνώστης μπορεί να καταφύγει στο παράρτημα Β′.

Υπενθυμίζουμε ότι ένας μεταθετικός δακτύλιος R με μονάδα λέγεται ακέραια περιοχή αν από κάθε σχέση της μορφής $xy = 0$ προκύπτει ότι $x = 0$ ή $y = 0$. (Βλέπε ορισμό Β′.14 του παραρτήματος Β′). Παρατηρούμε ότι ο $\mathbb{Z}_4$ δεν είναι ακέραια περιοχή, αφού $\langle 2\rangle\langle 2\rangle = \langle 2 \cdot 2\rangle = \langle 4\rangle = \langle 0\rangle$. Ο $\mathbb{Z}_2$ όμως είναι. Έχουμε το ακόλουθο θεώρημα:

Θεώρημα 2.46. Ο $\mathbb{Z}_n$ είναι ακέραια περιοχή αν και μόνον αν ο n είναι πρώτος.

Απόδειξη: Έστω ότι ο n είναι πρώτος. Έχουμε: $\langle x\rangle\langle y\rangle = \langle 0\rangle \Leftrightarrow \langle xy\rangle = \langle 0\rangle \Leftrightarrow xy \equiv 0 \mod n \Leftrightarrow$ $\Leftrightarrow n \mid xy \underset{n \text{ πρώτος}}{\Leftrightarrow} \big(n \mid x \text{ ή } n \mid y\big) \Leftrightarrow \big(x \equiv 0 \mod n \text{ ή } y \equiv 0 \mod n\big) \Leftrightarrow \big(\langle x\rangle = \langle 0\rangle \text{ ή } \langle y\rangle = \langle 0\rangle\big)$. Αντιστρόφως, έστω ότι ο n είναι σύνθετος. Τότε $n = n_1 n_2$, όπου $1 < n_1, n_2 < n$. Τότε $\langle n_1\rangle \neq \langle 0\rangle$ και $\langle n_2\rangle \neq \langle 0\rangle$. Αλλά $\langle n_1\rangle\langle n_2\rangle = \langle n_1 n_2\rangle = \langle n\rangle = \langle 0\rangle$. ■

Με βάση την πρόταση Β′.17 κάθε πεπερασμένη ακέραια περιοχή είναι σώμα, δηλαδή κάθε μη μηδενικό στοιχείο της αντιστρέφεται.

Πόρισμα 2.47. Ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα αν και μόνον αν ο n είναι πρώτος. Με βάση το «Μικρό» Θεώρημα του Fermat το αντίστροφο $\langle x\rangle^{-1}$ μιας μη μηδενικής κλάσης $\langle x\rangle$ είναι η κλάση $\langle x\rangle^{n-2} = \langle x^{n-2}\rangle$. ■

Ακόμη και στην περίπτωση που το n δεν είναι πρώτος, υπάρχουν αντιστρέψιμα στοιχεία στο $\mathbb{Z}_n$.

Πρόταση 2.48. Οι μόνες αντιστρέψιμες κλάσεις στον δακτύλιο $\mathbb{Z}_n$ είναι οι πρώτες προς το n.

Απόδειξη: Αν $(\alpha, n) = 1$, τότε σύμφωνα με την πρόταση 2.39 η ισοτιμία $\alpha x \equiv 1 \mod n$ έχει μοναδική λύση modulo n. Άρα $\langle\alpha\rangle\langle x\rangle = \langle 1\rangle$. Σύμφωνα μάλιστα με το πόρισμα 2.40, $\langle x\rangle = \langle\alpha\rangle^{-1} = \langle\alpha^{\varphi(n)-1}\rangle$. Σύμφωνα τώρα με το (ii) του θεωρήματος 2.41, η γραμμική ισοτιμία $\alpha x \equiv 1 \mod n$ έχει λύση αν και μόνον αν $(\alpha, n) \mid 1 \Leftrightarrow (\alpha, n) = 1$. ■

2.8 Αριθμητικές συναρτήσεις και ο τύπος αντιστροφής του Möbius

Ορισμός 2.49. Μια συνάρτηση $f : \mathbb{Z}_+ = \{1, 2, 3, \ldots\} \to \mathbb{R}$ ή $\mathbb{C}$ λέγεται αριθμητική συνάρτηση.

Για παράδειγμα, η συνάρτηση φ του Euler είναι μια αριθμητική συνάρτηση.
Τώρα, αν f είναι μια αριθμητική συνάρτηση, τότε μπορούμε να ορίσουμε μια νέα αριθμητική συνάρτηση F με τύπο

$$F(n) = \sum_{d|n} f(d),$$

όπου το άθροισμα εκτείνεται σ' όλους τους διαιρέτες του θετικού ακεραίου n.
Για παράδειγμα, $F(12) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$. Πολλές φορές είμαστε αναγκασμένοι να γράφουμε το ίδιο άθροισμα ανάποδα. Δηλαδή

$$F(n) = \sum_{d|n} f\Big(\frac{n}{d}\Big).$$

Αυτό δεν αλλάζει το τελικό αποτέλεσμα γιατί, καθώς το d διατρέχει όλους τους διαιρέτες του n, τότε και το $\dfrac{n}{d}$ διατρέχει επίσης (ανάποδα) όλους τους θετικούς διαιρέτες του n. Ας δούμε το προηγούμενο παράδειγμα. Αν πάρουμε τα διάφορα $\dfrac{12}{d}$, όπου το d διατρέχει όλους τους διαιρέτες του 12, τότε παίρνουμε τους αριθμούς $\dfrac{12}{1} = 12$, $\dfrac{12}{2} = 6$, $\dfrac{12}{3} = 4$, $\dfrac{12}{4} = 3$, $\dfrac{12}{6} = 2$ και τέλος $\dfrac{12}{12} = 1$. Άρα

$$f\Big(\frac{12}{1}\Big) + f\Big(\frac{12}{2}\Big) + f\Big(\frac{12}{3}\Big) + f\Big(\frac{12}{4}\Big) + f\Big(\frac{12}{6}\Big) + f\Big(\frac{12}{12}\Big) = f(12) + f(6) + f(4) + f(3) + f(2) + f(1),$$

που είναι το ίδιο με το άθροισμα $f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$. Γενικά λοιπόν ισχύει

$$\sum_{d|n} f(d) = \sum_{d|n} f\Big(\frac{n}{d}\Big).$$

Ορισμός 2.50. Μια αριθμητική συνάρτηση f λέγεται **πολλαπλασιαστική** αν για κάθε $m, n > 0$ με $(m, n) = 1$ ισχύει η σχέση

$$f(mn) = f(m)f(n).$$

Για παράδειγμα, η συνάρτηση φ του Euler είναι πολλαπλασιαστική.

Ορισμός 2.51. Μια αριθμητική συνάρτηση f λέγεται **πλήρως πολλαπλασιαστική** αν για κάθε $m, n > 0$ ισχύει η σχέση

$$f(mn) = f(m)f(n).$$

Για παράδειγμα, η συνάρτηση $N^\alpha : \mathbb{Z}_+ \to \mathbb{R}$, όπου $\alpha \in \mathbb{R}$, με $N^\alpha(n) = n^\alpha$, για κάθε θετικό ακέραιο n, είναι πλήρως πολλαπλασιαστική. Ειδικότερα οι συναρτήσεις $u = N^0$ και $N = N^1$ είναι πλήρως πολλαπλασιαστικές.
Μια πλήρως πολλαπλασιαστική συνάρτηση είναι προφανώς πολλαπλασιαστική. Το αντίστροφο δεν αληθεύει. Για παράδειγμα η συνάρτηση φ του Euler είναι πολλαπλασιαστική, αλλά όχι πλήρως πολλαπλασιαστική.

Πρόταση 2.52. Αν f είναι μια πολλαπλασιαστική συνάρτηση, τότε και η συνάρτηση F με τύπο

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

είναι πολλαπλασιαστική.
Απόδειξη: Έστω m και n θετικοί ακέραιοι με $(m, n) = 1$. Έστω $d \mid mn$. Θα αποδείξουμε πρώτα ότι το d γράφεται μονοσημάντως στη μορφή $d = d_1d_2$, όπου $d_1 \mid m$ και $d_2 \mid n$. Θέτουμε $d_1 = (d, m)$ και $d_2 = (d, n)$. Προφανώς $d_1 \mid m$ και $d_2 \mid n$. Επίσης $d = (d, mn) \mid (d, m)(d, n) = d_1d_2$. Από την άλλη μεριά, $d_1 = (d, m) \mid d$ και $d_2 = (d, n) \mid d$. Ακόμη $(d_1, d_2) \mid (m, n) = 1 \Rightarrow (d_1, d_2) = 1$. Συνεπώς $d_1d_2 \mid d$, για να καταλήξουμε τελικά $d = d_1d_2$. Αν τώρα $d = d_1d_2 = d_1'd_2'$, όπου $d_1' \mid m$ και $d_2' \mid n$, τότε $d_1 \mid d_1'd_2' \underset{(d_1, d_2')=1}{\Rightarrow} d_1 \mid d_1'$. Ανάλογα $d_1' \mid d_1$. Συνεπώς $d_1 = d_1'$ και επομένως και $d_2 = d_2'$.

Επομένως έχουμε:
$$F(mn)=\sum_{d|mn} f(d)=\sum_{\substack{d_1|m\\ d_2|n}} f(d_1d_2) \underset{(d_1,d_2)=1}{=} \sum_{\substack{d_1|m\\ d_2|n}} f(d_1)f(d_2)=\sum_{d_1|m} f(d_1)\cdot\sum_{d_2|n} f(d_2)=F(m)F(n). \qquad \blacksquare$$

Ορισμός 2.53. Αν $k\geq$ είναι ένας μη αρνητικός ακέραιος, ορίζουμε τις συναρτήσεις $\sigma_k=\sum_{d|n} d^k$.

Ειδικότερα, θέτουμε $\tau=\sigma_0$ και $\sigma=\sigma_1$.
Επομένως $\tau(n)=\sum_{d|n} 1=$ το πλήθος των διαιρετών του n και
$\sigma(n)=\sum_{d|n} d=$ το άθροισμα των διαιρετών του n.

Παρατηρούμε ότι $\tau(n)=\sum_{d|n} u(d)$ και $\sigma=\sum_{d|n} N(d)$.

Πόρισμα 2.54. Επειδή οι συναρτήσεις N^k είναι πλήρως πολλαπλασιαστικές, άρα πολλαπλασιαστικές, προκύπτει ότι και οι συναρτήσεις σ_k είναι πολλαπλασιαστικές. $\blacksquare$

Πρόταση 2.55. (i) $\tau(1)=1$ και $\tau(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\lambda^{\alpha_\lambda})=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_\lambda+1)$, όπου $\alpha_i>0$ και $p_i\neq p_j$ για $i\neq j$.

(ii) $\sigma_k(1)=1$ και $\sigma_k(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\lambda^{\alpha_\lambda})=\dfrac{p_1^{k(\alpha_1+1)}-1}{p_1^k-1}\cdot\dfrac{p_2^{k(\alpha_2+1)}-1}{p_2^k-1}\cdots\dfrac{p_\lambda^{k(\alpha_\lambda+1)}-1}{p_\lambda^k-1}$, για κάθε θετικό ακέραιο k. Ειδικότερα $\sigma(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\lambda^{\alpha_\lambda})=\dfrac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\dfrac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\dfrac{p_\lambda^{\alpha_\lambda+1}-1}{p_\lambda-1}$.

Απόδειξη: (i) Η περίπτωση $n=1$ είναι τετριμμένη. Έστω $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\lambda^{\alpha_\lambda}$, όπου $\alpha_i>0$ και $p_i\neq p_j$ για $i\neq j$. Κάθε διαιρέτης του n είναι της μορφής $p_1^{\beta_1}p_2^{\beta_2}\cdots p_\lambda^{\beta_\lambda}$, όπου $0\leq\beta_i\leq\alpha_i$. Επομένως έχουμε α_1+1 επιλογές για το β_1, α_2+1 επιλογές για το $\beta_2,\ldots,\alpha_\lambda+1$ επιλογές για το β_λ. Επομένως παίρνουμε $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_\lambda+1)$ διαιρέτες του n.
(ii) Πάλι η περίπτωση $n=1$ είναι τετριμμένη. Έστω $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\lambda^{\alpha_\lambda}$, όπως προηγουμένως και κάθε διαιρέτης του n είναι της μορφής $p_1^{\beta_1}p_2^{\beta_2}\cdots p_\lambda^{\beta_\lambda}$, όπου $0\leq\beta_i\leq\alpha_i$. Επομένως
$$\sigma_k(n)=\sum_{d|n} d^k=\sum_{\substack{i=1,2,\ldots,\lambda\\ 0\leq\beta_i\leq\alpha_i}} p_1^{k\beta_1}p_2^{k\beta_2}\cdots p_\lambda^{k\beta_\lambda}=\sum_{\beta_1=0}^{\alpha_1} p_1^{k\beta_1}\cdot\sum_{\beta_2=0}^{\alpha_2} p_2^{k\beta_2}\cdots\sum_{\beta_\lambda=0}^{\alpha_\lambda} p_\lambda^{k\beta_\lambda}=$$
$$=\frac{p_1^{k(\alpha_1+1)}-1}{p_1^k-1}\cdot\frac{p_2^{k(\alpha_2+1)}-1}{p_2^k-1}\cdots\frac{p_\lambda^{k(\alpha_\lambda+1)}-1}{p_\lambda^k-1}. \qquad \blacksquare$$

Παρατήρηση: Από τους τύπους των συναρτήσεων τ και σ_k μπορεί κανείς εύκολα να συμπεράνει ότι οι συναρτήσεις αυτές είναι πολλαπλασιαστικές, χωρίς να καταφύγει στην πρόταση 2.45.

Ορισμός 2.56. Ορίζουμε τη συνάρτηση $\mu:\mathbb{Z}_+\to\mathbb{Z}$ ως εξής:
$$\mu(n)=\begin{cases}1, & \text{αν } n=1\\ (-1)^k, & \text{αν } n=p_1p_2\cdots p_k, \text{ όπου } p_1,p_2,\ldots,p_k \text{ διακεκριμένοι πρώτοι}\\ 0, & \text{σε κάθε άλλη περίπτωση.}\end{cases}$$
Η συνάρτηση μ λέγεται **συνάρτηση του Möbius**.

Παρατηρούμε ότι η συνάρτηση του Möbius μηδενίζεται σ' εκείνα τα n, τα οποία διαιρούνται με το τετράγωνο πρώτου. Πράγματι η μ μηδενίζεται σ' έναν ακέραιο n αν αυτός διαιρείται από μια δύναμη p^t, όπου p πρώτος και $t\geq 2$. Αλλά τότε ο n θα διαιρείται από το p^2. Με βάση αυτή την παρατήρηση μπορεί κανείς εύκολα να αποδείξει ότι η συνάρτηση του Möbius είναι πολλαπλασιαστική.

Πρόταση 2.57. Η συνάρτηση του Möbius είναι πολλαπλασιαστική.
Απόδειξη: Έστω m και n θετικοί ακέραιοι με $(m,n)=1$. Αν $m=1$ ή $n=1$, π.χ. αν $m=1$ τότε προφανώς $\mu(mn)=\mu(m)\mu(n)$. $\big($Γιατί $\mu(mn)=\mu(1\cdot n)=\mu(n)=1\cdot\mu(n)\underset{m=1}{=}\mu(m)\mu(n)\big)$. Αν πάλι $p^2\mid mn$, για

κάποιον πρώτο p, τότε $p^2 \mid m$ ή $p^2 \mid n$. Αν $p^2 \mid m$, τότε $\mu(m) = 0$ και $\mu(m)\mu(n) = 0 \cdot \mu(n) = 0 = \mu(mn)$. Ομοίως αν $p^2 \mid n$. Τέλος, υποθέτουμε ότι $m = p_1 p_2 \cdots p_\kappa$ και $n = q_1 q_2 \cdots q_\lambda$, όπου $p_1, p_2, \ldots, p_\kappa, q_1, q_2, \ldots, q_\lambda$ διακεκριμένοι πρώτοι. Τότε $\mu(m)\mu(n) = (-1)^\kappa (-1)^\lambda = (-1)^{\kappa+\lambda} = \mu(p_1 p_2 \cdots p_\kappa q_1 q_2 \cdots q_\lambda) = \mu(mn)$. ■

Πρόταση 2.58. Ισχύει η σχέση: $\displaystyle\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & \text{αν } n = 1 \\ 0, & \text{αν } n > 1. \end{cases}$

1η Απόδειξη: Αν $n = 1$, ο μόνος διαιρέτης του n είναι ο εαυτός του (το 1) και άρα το άθροισμα ισούται με $\mu(1) = 1$. Έστω $n > 1$ και $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ η ανάλυση του n σε γινόμενο πρώτων παραγόντων. Οι μόνοι διαιρέτες του n, εκτός από το 1, που δεν διαιρούνται από τετράγωνο πρώτου είναι της μορφής $p_{i_1} p_{i_2} \cdots p_{i_s}$, όπου $1 \le i_1 < i_2 < \cdots < i_s \le k$. Η τιμή της μ σ' έναν τέτοιο διαιρέτη είναι $(-1)^s$. Υπάρχουν προφανώς $\binom{k}{s}$ τέτοιοι διαιρέτες. Το άθροισμα των τιμών της μ σ' όλους αυτούς τους διαιρέτες είναι λοιπόν $\binom{k}{s}(-1)^s$. Αν προσθέσουμε και το $1 = \mu(1)$ θα πάρουμε συνολικά

$$\sum_{d|n} \mu(d) = 1 - \binom{k}{1} + \binom{k}{2} - \cdots + \binom{n}{s}(-1)^s + \cdots + \binom{k}{k}(-1)^k = (1-1)^k = 0.$$

2η Απόδειξη: Εξετάζουμε μόνον την περίπτωση που $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} > 1$. Επειδή η μ είναι πολλαπλασιαστική, και η συνάρτηση $I(n) = \sum_{d|n} \mu(d)$ είναι πολλαπλασιαστική. Επομένως $I(n) = I(p_1^{\alpha_1}) I(p_2^{\alpha_2}) \cdots I(p_k^{\alpha_k}) =$

$$= \big(\mu(1) + \mu(p_1) + \underbrace{\mu(p_1^2) + \cdots}_{\text{μηδέν}}\big)\big(\mu(1) + \mu(p_2) + \underbrace{\mu(p_2^2) + \cdots}_{\text{μηδέν}}\big) \cdots \big(\mu(1) + \mu(p_k) + \underbrace{\mu(p_k^2) + \cdots}_{\text{μηδέν}}\big) =$$

$$= \underbrace{(1-1)(1-1)\cdots(1-1)}_{k \text{ παρενθέσεις}} = 0.$$ ■

Πρόταση 2.59. Ισχύει η σχέση: $\displaystyle\sum_{d|n} \varphi(d) = n$, για κάθε θετικό ακέραιο n.

Απόδειξη: Για κάθε διαιρέτη d του n ορίζουμε το σύνολο $\mathrm{A}_d = \{k \in \{1, 2, \ldots, n\} \mid (k, n) = d\}$. Υπολογίζουμε τώρα το πλήθος των στοιχείων του A_d. Έχουμε $k \in \mathrm{A}_d \Leftrightarrow (k, n) = d \Leftrightarrow \left(\frac{k}{d}, \frac{n}{d}\right) = 1$. Ακόμη $1 \le \frac{k}{d} \le \frac{n}{d}$. Επομένως ο $\frac{k}{d}$ είναι ένας από τους $\varphi\left(\frac{n}{d}\right)$ ακεραίους από το σύνολο $\left\{1, 2, \ldots, \frac{n}{d}\right\}$ που είναι πρώτοι προς τον $\frac{n}{d}$. Αντιστρόφως, έστω $\lambda \in \left\{1, 2, \ldots, \frac{n}{d}\right\}$ με $\left(\lambda, \frac{n}{d}\right) = 1$. Θεωρούμε τον ακέραιο $k = \lambda d \le \frac{n}{d} \cdot d = n$. Τότε $(k, n) = \left(\lambda d, \frac{n}{d} \cdot d\right) = d \cdot \left(\lambda, \frac{n}{d}\right) = d$, δηλαδή $k \in \mathrm{A}_d$. Επομένως το πλήθος των στοιχείων του A_d ισούται με το πλήθος των στοιχείων του $\left\{1, 2, \ldots, \frac{n}{d}\right\}$ που είναι πρώτα προς το $\frac{n}{d}$, δηλαδή $\varphi\left(\frac{n}{d}\right)$. Επειδή κάθε ακέραιος από το σύνολο $\{1, 2, \ldots, n\}$ ανήκει σε κάποιο A_d, για **μοναδικό** $d \mid n$, έπεται ότι $\sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} |\mathrm{A}_d| = n$. Αλλά, όπως είδαμε στην αρχή της παραγράφου, το άθροισμα $\sum_{d|n} \varphi\left(\frac{n}{d}\right)$ συμπίπτει με το άθροισμα $\sum_{d|n} \varphi(d)$. Επομένως $\sum_{d|n} \varphi(d) = n$. ■

Πριν προχωρήσουμε στα επόμενα, θα πρέπει πρώτα να ξεκαθαρίσουμε κάποια πράγματα τα οποία έχουν να κάνουν με τον συμβολισμό αθροισμάτων. Ας υποθέσουμε ότι έχουμε το άθροισμα

$$\sum_{ud|n} f(u)g(d).$$

Είναι προφανές ότι το άθροισμα εκτείνεται σ' όλα τα ζεύγη (u, d) των διαιρετών του n, των οποίων το γινόμενο διαιρεί επίσης το n. Επειδή η σχέση $ud \mid n$ είναι ισοδύναμη με τη σχέση $d \,\Big|\, \frac{n}{u}$, θα μπορούσαμε να επιλέξουμε πρώτα τον διαιρέτη u του n και στη συνέχεια τον d. Ο d όμως αναγκαστικά θα πρέπει να διαιρεί τον $\frac{n}{u}$. Επομένως το άθροισμα $\sum_{ud|n} f(u)g(d)$ μπορεί να γραφεί ισοδύναμα στη μορφή

$$\sum_{u|n}\sum_{d\,|\,\frac{n}{u}} f(u)g(d) = \sum_{u|n} f(u) \sum_{d\,|\,\frac{n}{u}} g(d).$$

Θα μπορούσαμε όμως να επιλέξουμε πρώτα τον διαιρέτη d και στη συνέχεια τον u, ο οποίος όμως θα πρέπει να διαιρεί τον $\dfrac{n}{d}$. Τότε το άθροισμα γράφεται στη μορφή

$$\sum_{d|n}\sum_{u\,|\,\frac{n}{d}} f(u)g(d) = \sum_{d|n} g(d) \sum_{u\,|\,\frac{n}{u}} f(u).$$

Οι τρεις μορφές του αθροίσματος είναι λοιπόν ισοδύναμες και συνεπώς έχουμε

$$\sum_{ud|n} f(u)g(d) = \sum_{u|n} f(u) \sum_{d\,|\,\frac{n}{u}} g(d) = \sum_{d|n} g(d) \sum_{u\,|\,\frac{n}{u}} f(u).$$

Θεώρημα 2.60. (Τύπος αντιστροφής του Möbius) Έστω f μια αριθμητική συνάρτηση. Ορίζουμε τη συνάρτηση F βάσει του τύπου

$$F(n) = \sum_{d|n} f(d) \quad .$$

Τότε ισχύει ο τύπος

$$f(n) = \sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) F(d).$$

Απόδειξη: Το ότι τα αθροίσματα $\sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big)$ και $\sum_{d|n} \mu\Big(\frac{n}{d}\Big) F(d)$ είναι ίσα προκύπτει, όπως έχουμε προαναφέρει από το γεγονός ότι καθώς το d διατρέχει όλους τους διαιρέτες του n, τότε και το $\dfrac{n}{d}$ διατρέχει επίσης όλους τους διαιρέτες του n. Αρκεί λοιπόν να αποδείξουμε ότι $\sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) = f(n)$.

Έχουμε: $\sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu(d) \sum_{u\,|\,\frac{n}{d}} f(u) = \sum_{ud|n} \mu(d) f(u) = \sum_{u|n} f(u) \sum_{d\,|\,\frac{n}{u}} \mu(d)$, σύμφωνα με τα προηγούμενα. Αλλά $\sum_{d\,|\,\frac{n}{u}} \mu(d) = \Big\lfloor \dfrac{1}{n/u} \Big\rfloor = \Big\lfloor \dfrac{u}{n} \Big\rfloor = \begin{cases} 1, & \text{αν } u = n \\ 0, & \text{αν } u < n \end{cases}$

Συνεπώς $$\sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) = \sum_{u|n} f(u) \sum_{d\,|\,\frac{n}{u}} \mu(d) = f(n) \cdot 1 = f(n).$$ ■

Πόρισμα 2.61. Ισχύει ο τύπος: $\varphi(n) = \sum_{d|n} \mu(d) \cdot \dfrac{n}{d} = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \cdot d.$

Απόδειξη: Με βάση την πρόταση 2.59 έχουμε $\sum_{d|n} \varphi(d) = n = N(n)$. Σύμφωνα με τον τύπο αντιστροφής του Möbius έχουμε: $\varphi(n) = \sum_{d|n} \mu(d) N\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu(d) \cdot \dfrac{n}{d}.$ ■

Με βάση το προηγούμενο πόρισμα μπορούμε να υπολογίσουμε ξανά τον τύπο της συνάρτησης φ του Euler. Επειδή η περίπτωση $\varphi(1) = 1$ δεν παρουσιάζει ενδιαφέρον, υποθέτουμε ότι $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} > 1$ είναι η ανάλυση του n σε γινόμενο πρώτων παραγόντων.
Οι μόνοι διαιρέτες του n στους οποίους η συνάρτηση μ δεν μηδενίζεται είναι το 1 και οι διαιρέτες της μορφής $p_{i_1} p_{i_2} \cdots p_{i_s}$, όπου $1 \le i_1 < i_2 < \cdots < i_s \le k$. Για δεδομένο s με $1 \le s \le k$ υπάρχουν $\binom{k}{s}$ τέτοιοι διαιρέτες, στους οποίους η συνάρτηση μ παίρνει την τιμή $(-1)^s$. Επομένως

$$\varphi(n) = 1 \cdot n + \sum_{1\le i\le k} \mu(p_i) \cdot \frac{n}{p_i} + \sum_{1\le i_1<i_2\le k} \mu(p_{i_1}p_{i_2}) \cdot \frac{n}{p_{i_1}p_{i_2}} + \sum_{1\le i_1<i_2<i_3\le k} \mu(p_{i_1}p_{i_2}p_{i_3}) \cdot \frac{n}{p_{i_1}p_{i_2}p_{i_3}} + \cdots +$$

$$+\mu(p_1p_2\cdots p_k) \cdot \frac{n}{p_1p_2\cdots p_k} = n - \sum_{1\le i\le k} \frac{n}{p_i} + \sum_{1\le i_1<i_2\le k} \frac{n}{p_{i_1}p_{i_2}} - \sum_{1\le i_1<i_2<i_3\le k} \frac{n}{p_{i_1}p_{i_2}p_{i_3}} + \cdots (-1)^k \frac{n}{p_1p_2\cdots p_k} =$$

$$= n\Bigg(1 - \sum_{1\le i\le k} \frac{1}{p_i} + \sum_{1\le i_1<i_2\le k} \frac{1}{p_{i_1}p_{i_2}} - \sum_{1\le i_1<i_2<i_3\le k} \frac{1}{p_{i_1}p_{i_2}p_{i_3}} + \cdots (-1)^k \frac{1}{p_1p_2\cdots p_k}\Bigg) =$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

Ορισμός 2.62. Ένας θετικός ακέραιος n λέγεται **τέλειος** αν ισούται με το άθροισμα των γνήσιων διαιρετών του, δηλαδή αυτών που είναι μικρότεροι από τον n. Ισοδύναμα, ο n είναι τέλειος αν και μόνον αν $\sigma(n)=2n$.

Για παράδειγμα, οι αριθμοί 6, 28, 496 είναι τέλειοι. Μέχρι τώρα δεν έχουν βρεθεί περιττοί τέλειοι αριθμοί. Για τους άρτιους τέλειους αριθμούς έχουμε την επόμενη πρόταση:

Πρόταση 2.63. Έστω n ένας άρτιος αριθμός. Τότε ο n είναι τέλειος αν και μόνον αν είναι της μορφής $2^{p-1}(2^p-1)$, όπου p πρώτος και 2^p-1 πρώτος αριθμός Mersenne.

Απόδειξη: Εφόσον ο n είναι άρτιος, θα είναι της μορφής $n=2^r\cdot\lambda$, όπου λ περιττός. Τότε $2^{r+1}\lambda=2n=$ $=\sigma(n)=\sigma(2^r)\sigma(\lambda)$. Αλλά $\sigma(2^r)=1+2+2^2+\cdots+2^r=2^{r+1}-1$. Επομένως έχουμε τη σχέση $2^{r+1}\cdot\lambda=(2^{r+1}-1)\sigma(\lambda)$. Επειδή $(2^{r+1},2^{r+1}-1)=1$ και $2^{r+1}\mid(2^{r+1}-1)\sigma(\lambda)$, έπεται ότι $2^{r+1}\mid\sigma(\lambda)$. Έστω $\sigma(\lambda)=\mu\cdot 2^{r+1}$. Τότε $\lambda=\mu(2^{r+1}-1)$.
Αν $\mu>1$, τότε το $\lambda=\mu(2^{r+1}-1)$ θα είχε τρεις τουλάχιστον διαφορετικούς διαιρέτες. Το 1, το μ και το $\mu(2^{r+1}-1)=\lambda$. Επομένως $1+\mu+\lambda\le\sigma(\lambda)$ και άρα $2^{r+1}\lambda=(2^{r+1}-1)\sigma(\lambda)\ge(2^{r+1}-1)(1+\mu+\lambda)\Rightarrow$ $\Rightarrow 2^{r+1}\lambda\ge(2^{r+1}-1)(1+\mu)+2^{r+1}\lambda-\lambda\Leftrightarrow\lambda\ge(2^{r+1}-1)(1+\mu)>(2^{r+1}-1)\mu=\lambda$, άτοπο. Άρα $\mu=1$.
Επομένως $\lambda=2^{r+1}-1$ και $\sigma(\lambda)=2^{r+1}=2^{r+1}-1+1=\lambda+1$. Επειδή $\sigma(\lambda)=\lambda+1$, ο λ είναι πρώτος. Άρα είναι ένας πρώτος του Mersenne της μορφής $M_p=2^p-1$, όπου p πρώτος. Συνεπώς $r+1=p\Leftrightarrow r=p-1$.
Ο n γράφεται τελικά στη μορφή $n=2^{p-1}M_p=2^{p-1}(2^p-1)$.
Αντιστρόφως, υποθέτουμε ότι $n=2^{p-1}M_p$, όπου $M_p=2^p-1$ είναι ένας πρώτος αριθμός Mersenne. Τότε $\sigma(n)=\sigma(2^{p-1})\sigma(M_p)=(2^p-1)(M_p+1)=M_p\cdot 2^p=2(2^{p-1}M_p)=2n$. ■

Άσκηση 99. Το τελευταίο ψηφίο ενός αρτίου τέλειου αριθμού είναι το 6 ή το 8. Αν είναι το 8, τότε ο αριθμός λήγει σε 28.

Απόδειξη: Αν $n=2\cdot M_2=2(2^2-1)=6$, το συμπέρασμα ισχύει. Έστω $n=2^{p-1}M_p=2^{p-1}(2^p-1)$, όπου M_p πρώτος αριθμός Mersenne και $p\ge 3$. Τότε ο p είναι της μορφής $p=4k+1$ ή $p=4k+3$, όπου k θετικός ακέραιος. $\big($Οι περιπτώσεις $p=4k$ και $p=4k+2$ αποκλείονται γιατί $2\nmid p\big)$.
Παρατηρούμε ότι $2^4=16\equiv 6 \mod 10$. Έστω $2^{4k}\equiv 6 \mod 10$, για κάποιον θετικό ακέραιο k. Τότε $2^{4(k+1)}=2^{4k}\cdot 2^4=2^{4k}\cdot 16\equiv 6\cdot 6=36\equiv 6 \mod 10$. Επαγωγικά συμπεραίνουμε ότι $2^{4k}\equiv 6 \mod 10$, για κάθε θετικό ακέραιο k. Επομένως $2^{4k}(2^{4k+1}-1)=2^{4k}(2^{4k}\cdot 2-1)\equiv 6(6\cdot 2-1)=6\cdot 11=66\equiv 6 \mod 10$.
Η περίπτωση λοιπόν $p=2k+1$ έχει καλυφθεί.
Έστω τώρα $p=4k+3$, όπου k θετικός ακέραιος. Παρατηρούμε ότι $2^{4k}=16^k\equiv(-9)^k \mod 25$. Άρα $2^{4k}(2^{4k+3}-1)=2^{4k}(8\cdot 2^{4k}-1)\equiv(-9)^k(8(-9)^k-1)=8(-9)^{2k}-(-9)^k \mod 25$. Πολλαπλασιάζοντας επί 4 παίρνουμε $2^{4k+2}(2^{4k+3}-1)=4\cdot 2^{4k}(2^{4k+3}-1)\equiv 4\cdot(8(-9)^{2k}-(-9)^k)=32(-9)^{2k}-4(-9)^k \mod 100$.
Παρατηρούμε ότι $(-9)^r-1=-10((-9)^{r-1}+(-9)^{r-2}+\cdots+(-9)+1)$, για κάθε θετικό ακέραιο r. Επίσης $(-9)^{r-1}+(-9)^{r-2}+\cdots+(-9)+1\equiv 1^{r-1}+1^{r-2}+\cdots+1\equiv r \mod 10\Rightarrow 10((-9)^{r-1}+(-9)^{r-2}+\cdots+$ $+(-9)+1)\equiv 10r \mod 100\Leftrightarrow -10((-9)^{r-1}+(-9)^{r-2}+\cdots+(-9)+1)\equiv -10r \mod 100\Leftrightarrow(-9)^r-1\equiv$ $\equiv -10r \mod 100\Leftrightarrow(-9)^r\equiv 1-10r \mod 100$.
Επομένως $32(-9)^{2k}-4(-9)^k\equiv 32(1-10\cdot 2k)-4(1-10k)=32-640k-4+40k=28-600k\equiv 28 \mod 100$. ■

Μια άλλη απόδειξη ότι $2^{4k+2}(2^{4k+3}-1)\equiv 28 \mod 100$ στηρίζεται στην ακόλουθη παρατήρηση:

$$\begin{cases}(-9)^1\equiv -9\equiv 16\equiv 25+16=\boxed{41} \mod 25\\ (-9)^2=81\equiv 6\equiv 25+6=\boxed{31} \mod 25\\ (-9)^3\equiv 6(-9)=-54\equiv -4\equiv 25-4=\boxed{21} \mod 25\\ (-9)^4\equiv 6^2=36\equiv\boxed{11} \mod 25\\ (-9)^5\equiv -99=-100+1\equiv\boxed{1} \mod 25\end{cases}$$

Παρατηρούμε ότι καθώς ο εκθέτης του -9 αυξάνει κατά 1, το ψηφίο των δεκάδων μειώνεται κατά 1. Επειδή $41=(5-1)10+1$, $31=(5-2)10+1$, $21=(5-3)10+1$, $11=(5-4)10+1$, $1=(5-5)10+1$, δημιουργείται

η εικασία μήπως $(-9)^k \equiv (5-k)10+1 = 1-10k+50 \equiv 1-10k \mod 25$. Αποδεικνύουμε με επαγωγή την εικασία αυτή.
Για $k=1$ έχουμε $-9 \equiv -9 \mod 25$, που ισχύει. Έστω ότι $(-9)^k \equiv 1-10k \mod 25$, για κάποιον θετικό ακέραιο k. Τότε $(-9)^{k+1} = -9(-9)^k \equiv -9(1-10k) = -9+90k = -9+100k-10k \equiv -9-10k = = 10-9-10k-10 = 1-10(k+1) \mod 25$ και η απόδειξη ολοκληρώθηκε.
Με βάση ότι $(-9)^k \equiv 1-10k \mod 25$ έχουμε: $2^{4k+2}(2^{4k+3}-1) = 4\cdot(2^4)^k(8\cdot(2^4)^k-1) \equiv 4(-9)^k(8(-9)^k- -1) = 32(-9)^{2k} - 4(-9)^k \equiv 7(-9)^{2k} - 4(-9)^k \equiv 7(1-10\cdot 2k) - 4(1-10k) = 3-100k \equiv 3 \mod 25$. Αν λοιπόν θέσουμε $x = 2^{4k+2}(2^{4k+3}-1)$, θα έχουμε το σύστημα των ισοτιμιών

$$\begin{cases} x \equiv 3 \mod 25 \\ x \equiv 0 \mod 4 \end{cases}$$

Από το κινεζικό θεώρημα, λύνουμε τις ισοτιμίες $4x \equiv 3 \mod 25 \underset{(6,25)=1}{\Leftrightarrow} 24x \equiv 18 \equiv -7 \mod 25 \Leftrightarrow -x \equiv -7 \mod 25 \Leftrightarrow x \equiv 7 \mod 25$ και $25x \equiv 0 \mod 4 \Leftrightarrow x \equiv 0 \mod 4$. Ο x είναι λοιπόν ισοϋπόλοιπος modulo 100 με τον $4\cdot 7 + 25\cdot 0 = 28$.

2.9 Πολυωνυμικές ισοτιμίες

2.10 Λύσεις των ασκήσεων του κεφαλαίου 2

Μέρος ΙΙ

Παραρτήματα

Παράρτημα Α΄

Σύνολα και συναφείς έννοιες

Στα μαθηματικά χρησιμοποιούμε σχεδόν παντού την έννοια του **συνόλου**. Είτε μιλάμε για σύνολα αριθμών, είτε για σύνολα συναρτήσεων είτε για διανυσματικούς χώρους ή άλλες αλγεβρικές δομές, πάντοτε θα καταφεύγουμε στην έννοια του συνόλου. Το σύνολο των αντικειμένων-εννοιών είναι το πλαίσιο στο οποίο κινείται κάθε μαθηματική θεωρία. Για να είμαστε ακριβείς σ᾽ αυτά που ορίζουμε και λέμε το πλαίσιο-σύνολο των εννοιών θα πρέπει να είναι σαφώς καθορισμένο. Αυτή καθεαυτή η έννοια του συνόλου είναι λοιπόν πρωταρχική έννοια. Ως πρωταρχική έννοια δεν είναι δυνατόν να οριστεί με τη βοήθεια άλλων πιο πρωταρχικών εννοιών. Είναι όπως, για παράδειγμα η έννοια του σημείου στη Γεωμετρία. Γι᾽ αυτό και δεν υπάρχει ορισμός για την έννοια του συνόλου.
Εμείς θα αρκεστούμε στη διαισθητική αντίληψη ότι σύνολο είναι μια συλλογή από κάποια αντικείμενα σαφώς καθορισμένα. Στην παραπάνω φράση έχουμε απλώς αντικαταστήσει τη λέξη «σύνολο» με τη λέξη «συλλογή». Άρα στην ουσία δεν έχουμε δώσει κανέναν ορισμό για την έννοια του συνόλου.
Τα σύνολα συνήθως τα παριστάνουμε με κεφαλαία γράμματα του ελληνικού ή λατινικού αλφαβήτου.

Ένα σύνολο μπορεί να παρασταθεί κατά δύο τρόπους:
α) Με **αναγραφή** των στοιχείων του. Έτσι, γράφουμε $\mathrm{A} = \{1, 3, 5, 7, 9\}$ ή $\mathrm{B} = \{\alpha, \varepsilon, \eta, \iota, o, \upsilon, \omega\}$ ή
β) με **περιγραφή** των στοιχείων του, δηλαδή γράφουμε $\{x \mid \text{το } x \text{ έχει την ιδιότητα } p\}$. Έτσι, στα προηγούμενα παραδείγματα μπορούμε να γράψουμε $\mathrm{A} = \{x \mid \text{το } x \text{ είναι θετικός περιττός ακέραιος μικρότερος του } 10\}$ και $\mathrm{B} = \{x \mid \text{το } x \text{ είναι φωνήεν του ελληνικού αλφαβήτου}\}$. Συνήθως η παράσταση ενός συνόλου με περιγραφή είναι προτιμητέα όταν το σύνολο είναι άπειρο. Υπάρχουν και εξαιρέσεις. Για παράδειγμα, γράφουμε $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ και οι τελείες υπονοούν τα στοιχεία που λείπουν.

Για να δηλώσουμε ότι το x είναι στοιχείο του συνόλου Α γράφουμε $x \in \mathrm{A}$ και διαβάζουμε **το x ανήκει στο Α**. Για λόγους ευελιξίας, όταν είμαστε αναγκασμένοι να γράψουμε πρώτα το σύνολο και μετά το στοιχείο γράφουμε $\mathrm{A} \ni x$ και διαβάζουμε **το Α περιέχει το x**.

Ορισμός Α΄.1. Δύο σύνολα Α και Β λέγονται **ίσα** αν περιέχουν τα ίδια ακριβώς στοιχεία. Δηλαδή $\mathrm{A} = \mathrm{B}$ αν και μόνον αν, για κάθε x ισχύει η ισοδυναμία: $x \in \mathrm{A} \Leftrightarrow x \in \mathrm{B}$.

Ορισμός Α΄.2. Αν Α και Β είναι δύο σύνολα, τότε το Α λέγεται **υποσύνολο** του Β ή ισοδύναμα ότι το Β είναι **υπερσύνολο** του Α, αν και μόνον αν κάθε στοιχείο του Α είναι και στοιχείο του Β. Σ᾽ αυτή την περίπτωση γράφουμε $\mathrm{A} \subseteq \mathrm{B}$ ή ισοδύναμα $\mathrm{B} \supseteq \mathrm{A}$. Δηλαδή $\mathrm{A} \subseteq \mathrm{B}$ αν και μόνον αν, για κάθε x ισχύει η συνεπαγωγή: $x \in \mathrm{A} \Rightarrow x \in \mathrm{B}$. Αν $\mathrm{A} \subseteq \mathrm{B}$ και $\mathrm{A} \neq \mathrm{B}$, τότε το Α λέγεται **γνήσιο υποσύνολο** του Β ή ισοδύναμα το Β **γνήσιο υπερσύνολο** του Α. Αυτό το συμβολίζουμε με $\mathrm{A} \subsetneq \mathrm{B}$ ή ισοδύναμα $\mathrm{B} \supsetneq \mathrm{A}$.

Πόρισμα Α΄.3. Αν Α και Β είναι δύο σύνολα, τότε $\mathrm{A} = \mathrm{B} \Leftrightarrow (\mathrm{A} \subseteq \mathrm{B}$ και $\mathrm{B} \subseteq \mathrm{A})$.

Ορισμός Α΄.4. Δεχόμαστε την ύπαρξη ενός συνόλου, το οποίο παριστάνουμε με $\varnothing$ και το οποίο δεν περιέχει στοιχεία. Το σύνολο αυτό λέγεται το **κενό** σύνολο. Για παράδειγμα, $\{x \in \mathbb{Q} \mid \ x^2 = 2\} = \varnothing$.

Πρόταση Α΄.5. **(i)** Αν $\mathrm{A} \subseteq \mathrm{B}$ και $\mathrm{B} \subseteq \Gamma$, τότε $\mathrm{A} \subseteq \Gamma$, **(ii)** $\varnothing \subseteq \mathrm{A}$, για κάθε σύνολο Α και **(iii)** Αν $\mathrm{A} \subseteq \varnothing$, τότε $\mathrm{A} = \varnothing$.

Απόδειξη: (i) Έχουμε: $x \in A \underset{A\subseteq B}{\Rightarrow} x \in B \underset{B\subseteq\Gamma}{\Rightarrow} x \in \Gamma$.
(ii) Αν $\varnothing \not\subseteq A$, τότε θα υπήρχε $x \in \varnothing$ με $x \notin A$. Αυτό είναι άτοπο γιατί δεν υπάρχει στοιχείο x, με $x \in \varnothing$.
(iii) Αν $A \neq \varnothing$, τότε θα υπήρχε $x \in A \underset{A\subseteq\varnothing}{\Rightarrow} x \in \varnothing$, άτοπο. ■

Ορισμός Α΄.6. Αν Α και Β είναι δύο σύνολα, τότε η **ένωσή** τους $A \cup B$ είναι το σύνολο όλων των στοιχείων του Α και όλων των στοιχείων του Β. Δηλαδή, $A \cup B = \{x \mid x \in A \text{ ή } x \in B\}$. Δηλαδή ισχύει η ισοδυναμία: $x \in A \cup B \Leftrightarrow (x \in A \text{ ή } x \in B)$.

Πρόταση Α΄.7. (i) $A \cup B = B \cup A$. **(ii)** $A \cup A = A$. **(iii)** $A \subseteq A \cup B$ και $B \subseteq A \cup B$.
(iv) $A \cup \varnothing = A$. **(v)** Αν $A \subseteq \Gamma$ και $B \subseteq \Gamma$, τότε $A \cup B \subseteq \Gamma$. **(vi)** $A \cup B = A \Leftrightarrow B \subseteq A$.
(vii) Αν $A \subseteq A_1$ και $B \subseteq B_1$, τότε $A \cup B \subseteq A_1 \cup B_1$. **(viii)** $(A \cup B) \cup \Gamma = A \cup (B \cup \Gamma)$, για κάθε τρία σύνολα Α, Β και Γ.
Απόδειξη: (i) $x \in A \cup B \Leftrightarrow (x \in A \text{ ή } x \in B) \Leftrightarrow (x \in B \text{ ή } x \in A) \Leftrightarrow x \in B \cup A$. **(ii)** $x \in A \cup A \Leftrightarrow$ $\Leftrightarrow (x \in A \text{ ή } x \in A) \Leftrightarrow x \in A$. **(iii)** $x \in A \Rightarrow (x \in A \text{ ή } x \in B) \Leftrightarrow x \in A \cup B$. Ομοίως $B \subseteq A \cup B$.
(iv) $x \in A \cup \varnothing \Leftrightarrow (x \in A \text{ ή } \underbrace{x \in \varnothing}_{\text{ψευδής}}) \Leftrightarrow x \in A$. **(v)** Έστω $x \in A \cup B$. Τότε $x \in A$ ή $x \in B$. Αν $x \in A \subseteq \Gamma$, τότε $x \in \Gamma$. Ομοίως, αν $x \in B \subseteq \Gamma$, τότε $x \in \Gamma$. Σε κάθε περίπτωση λοιπόν $x \in \Gamma$ και κατά συνέπεια, ισχύει η συνεπαγωγή $x \in A \cup B \Rightarrow x \in \Gamma$. **(vi)** Με βάση το προηγούμενο, όπου $\Gamma = A \cup B$, έχουμε: Αν $B \subseteq A$, τότε επειδή και $A \subseteq A$, θα έχουμε $A \cup B \subseteq A$. Αλλά από το (iii) $A \subseteq A \cup B$. Άρα $A \cup B = A$. Αντιστρόφως, έστω $A \cup B = A$. Τότε $B \subseteq A \cup B = A$. **(vii)** $A \subseteq A_1 \subseteq A_1 \cup B_1$ και $B \subseteq B_1 \subseteq A_1 \cup B_1$. Από το (v), για $\Gamma = A_1 \cup B_1$, παίρνουμε $A \cup B \subseteq A_1 \cup B_1$. **(viii)** $A \subseteq A \cup (B \cup \Gamma)$ και $B \subseteq B \cup \Gamma \subseteq A \cup (B \cup \Gamma)$. Άρα $A \cup B \subseteq A \cup (B \cup \Gamma)$. Επίσης, $\Gamma \subseteq B \cup \Gamma \subseteq A \cup (B \cup \Gamma)$. Επομένως $(A \cup B) \cup \Gamma \subseteq A \cup (B \cup \Gamma)$. Αντιστρόφως, $A \subseteq A \cup B \subseteq (A \cup B) \cup \Gamma$. Επίσης, $B \subseteq A \cup B \subseteq (A \cup B) \cup \Gamma$ και $\Gamma \subseteq (A \cup B) \cup \Gamma$. Άρα $B \cup \Gamma \subseteq (A \cup B) \cup \Gamma$. Επειδή $A \subseteq (A \cup B) \cup \Gamma$ και $B \cup \Gamma \subseteq (A \cup B) \cup \Gamma$, έπεται ότι $A \cup (B \cup \Gamma) \subseteq (A \cup B) \cup \Gamma$. Εναλλακτικά, $x \in (A \cup B) \cup \Gamma \Leftrightarrow (x \in A \cup B \text{ ή } x \in \Gamma) \Leftrightarrow ((x \in A \text{ ή } x \in B) \text{ ή } x \in \Gamma) \Leftrightarrow (x \in A \text{ ή } x \in B \text{ ή } x \in \Gamma) \Leftrightarrow (x \in$ $\in A \text{ ή } (x \in B \text{ ή } x \in \Gamma)) \Leftrightarrow (x \in A \text{ ή } x \in B \cup \Gamma) \Leftrightarrow x \in A \cup (B \cup \Gamma)$. ■

Ορισμός Α΄.8. Αν Α και Β είναι δύο σύνολα, τότε η **τομή** τους $A \cap B$ είναι το σύνολο των **κοινών** στοιχείων του Α και του Β. Δηλαδή, $A \cap B = \{x \mid x \in A \textbf{ και } x \in B\}$. Δηλαδή ισχύει η ισοδυναμία: $x \in A \cap B \Leftrightarrow$ $\Leftrightarrow (x \in A \text{ και } x \in B)$. Δύο σύνολα Α και Β λέγονται (μεταξύ τους) **ξένα** αν $A \cap B = \varnothing$.

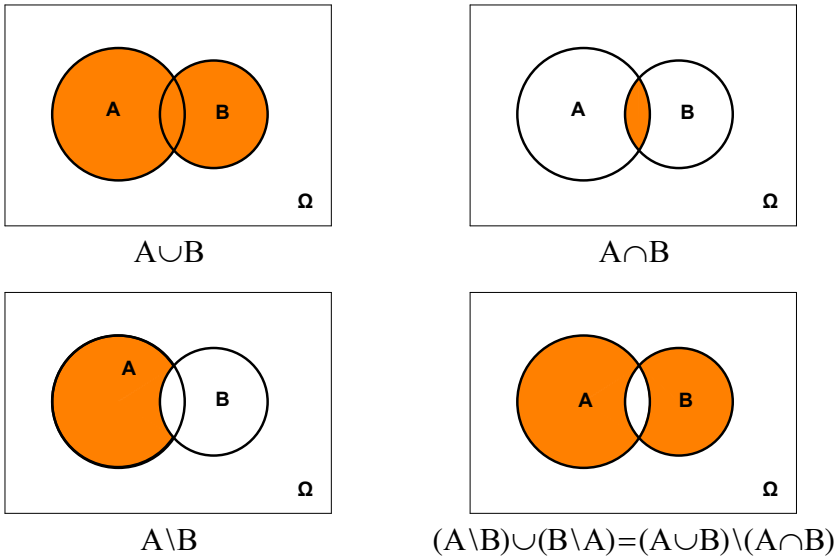
Πρόταση Α΄.9. (i) $A \cap B = B \cap A$. **(ii)** $A \cap A = A$. **(iii)** $A \cap B \subseteq A$ και $A \cap B \subseteq B$.
(iv) $A \cap \varnothing = \varnothing$. **(v)** Αν $\Gamma \subseteq A$ και $\Gamma \subseteq B$, τότε $\Gamma \subseteq A \cap B$. **(vi)** $A \cap B = A \Leftrightarrow A \subseteq B$.
(vii) Αν $A \subseteq A_1$ και $B \subseteq B_1$, τότε $A \cap B \subseteq A_1 \cap B_1$.
(viii) $(A \cap B) \cap \Gamma = A \cap (B \cap \Gamma)$, για κάθε τρία σύνολα Α, Β και Γ.
(ix) $A \cap (B \cup \Gamma) = (A \cap B) \cup (A \cap \Gamma)$, για κάθε τρία σύνολα Α, Β και Γ.
(x) $A \cup (B \cap \Gamma) = (A \cup B) \cap (A \cup \Gamma)$, για κάθε τρία σύνολα Α, Β και Γ.
Απόδειξη: Αποδεικνύουμε μόνον την **(ix)**, αφήνοντας τις υπόλοιπες ως άσκηση.
Αν $x \in A \cap (B \cup \Gamma)$, τότε $x \in A$ και $x \in B \cup \Gamma \Leftrightarrow (x \in B \text{ ή } x \in \Gamma)$. Αν $x \in B$, τότε (επειδή $x \in A$) $x \in A \cap B \subseteq$ $\subseteq (A \cap B) \cup (A \cap \Gamma)$. Ομοίως, αν $x \in \Gamma$, τότε $x \in A \cap \Gamma \subseteq (A \cap B) \cup (A \cap \Gamma)$. Σε κάθε περίπτωση $x \in (A \cap B) \cup (A \cap \Gamma)$. Άρα $A \cap (B \cup \Gamma) \subseteq (A \cap B) \cup (A \cap \Gamma)$. Αντιστρόφως, έστω $x \in (A \cap B) \cup (A \cap \Gamma) \Leftrightarrow (x \in A \cap B \text{ ή } x \in A \cap \Gamma)$. Αν $x \in A \cap B \Leftrightarrow (x \in A \text{ και } x \in B) \underset{B\subseteq B\cup\Gamma}{\Rightarrow} (x \in A \text{ και } x \in B \cup \Gamma) \Leftrightarrow x \in A \cap (B \cup \Gamma)$. Ομοίως, αν $x \in A \cap \Gamma$, τότε $x \in A \cap (B \cup \Gamma)$. Άρα $x \in (A \cap B) \cup (A \cap \Gamma) \Rightarrow x \in A \cap (B \cup \Gamma)$, δηλαδή $(A \cap B) \cup (A \cap \Gamma) \subseteq A \cap (B \cup \Gamma)$. ■

Ορισμός Α΄.10. Έστω Α και Β δύο σύνολα. Η **συνολοθεωρητική διαφορά** $A \setminus B$ είναι **το σύνολο των στοιχείων του Α που δεν ανήκουν στο Β**. Δηλαδή $A \setminus B = \{x \in A \mid x \notin B\}$.

Πρόταση Α΄.11. (i) $A \setminus B \subseteq A$. **(ii)** $A \setminus A = \varnothing$. **(iii)** $A \setminus B = A \Leftrightarrow A \cap B = \varnothing$.
(iv) $A \setminus B = \varnothing \Leftrightarrow A \subseteq B$. **(v)** $A \setminus B = A \setminus (A \cap B)$. **(vi)** $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.
(vii) $(A \setminus B) \cap (B \setminus A) = \varnothing$. **(viii)** $(A \setminus B) \cap (A \cap B) = (B \setminus A) \cap (A \cap B) = ((A \setminus B) \cup (B \setminus A)) \cap (A \cap B) = \varnothing$.
Απόδειξη: (i) Άμεση, από τον ορισμό της διαφοράς $A \setminus B$.
(ii) Αν $A \setminus A \neq \varnothing$, τότε θα υπήρχε $x \in A \setminus A$, δηλαδή $x \in A$ με $x \notin A$, αντίφαση.

(iii) Έστω $A \setminus B = A$. Υποθέτουμε ότι $A \cap B \neq \varnothing$, δηλαδή υπάρχει x, με $x \in A$ και $x \in B$. Εφόσον $x \in B$, $x \notin \{x \in A \mid \ x \notin B\} = A \setminus B = A$, αντίφαση. Άρα $A \cap B = \varnothing$. Αντιστρόφως, έστω $A \cap B = \varnothing$. Τότε, για κάθε $x \in A$ θα είχαμε $x \notin B$. Γιατί, σε αντίθετη περίπτωση θα υπήρχε $x \in A$, με $x \in B$, δηλαδή $x \in A \cap B = \varnothing$, άτοπο. Άρα $A \subseteq \{x \in A \mid \ x \notin B\} = A \setminus B \subseteq A$, ήτοι $A = A \setminus B$.
(iv) Έστω $A \setminus B = \varnothing$. Αν $A \not\subseteq B$, τότε θα υπήρχε $x \in A$ με $x \notin B$, ήτοι $x \in A \setminus B = \varnothing$, άτοπο. Άρα $A \subseteq B$. Αντιστρόφως, έστω $A \subseteq B$. Υποθέτουμε ότι $A \setminus B \neq \varnothing$, δηλαδή υπάρχει $x \in A$, με $x \notin B$. Επειδή όμως $A \subseteq B$, το x θα ανήκε στο B, αντίφαση. Άρα $A \setminus B = \varnothing$.
(v) Έστω $x \in A \setminus B$. Τότε $x \in A$ και $x \notin B$. Αν $x \in A \cap B \subseteq B$, τότε το x θα ήταν στοιχείο του B, άτοπο. Άρα $x \notin A \cap B$ και επειδή $x \in A$, $x \in A \setminus (A \cap B)$. Αντιστρόφως, έστω $x \in A \setminus (A \cap B)$. Τότε $x \in A$, οπότε αν $x \in B$, θα είχαμε $x \in A \cap B$, άτοπο. Άρα $x \notin B$ και συνεπώς $x \in A \setminus B$.
(vi) Έστω $x \in (A \setminus B) \cup (B \setminus A) \subseteq A \cup B$. Αν $x \in A \setminus B = \{x \in A \mid \ x \notin B\}$, τότε $x \notin A \cap B \subseteq B$. Ομοίως, αν $x \in B \setminus A$, τότε $x \notin A \cap B \subseteq A$. Σε κάθε περίπτωση $x \notin A \cap B$, ενώ $x \in A \cup B$. Άρα $x \in (A \cup B) \setminus (A \cap B)$. Αντιστρόφως, έστω $x \in (A \cup B) \setminus (A \cap B) \subseteq A \cup B$. Αν $x \in A$, τότε $x \notin B$, γιατί σε αντίθετη περίπτωση $x \in A \cap B$, άτοπο. Άρα $x \in A \setminus B$. Ομοίως, αν $x \in B$, τότε $x \in B \setminus A$. Άρα $(x \in A \setminus B$ ή $x \in B \setminus A) \Leftrightarrow x \in (A \setminus B) \cup (B \setminus A)$.
(vii) Έστω ότι υπάρχει x, με $x \in (A \setminus B) \cap (B \setminus A)$. Τότε $x \in A \setminus B$, άρα α) $x \in A$ και β) $x \notin B$. Επίσης, $x \in B \setminus A$, άρα γ) $x \in B$ και δ) $x \notin A$. Οι σχέσεις α) και δ) (ή οι σχέσεις β) και γ)) συνιστούν αντίφαση. Συνεπώς τέτοιο x δεν υπάρχει, ήτοι $(A \setminus B) \cap (B \setminus A) = \varnothing$.
(viii) $(A \setminus B) \cap (A \cap B) \subseteq (A \setminus B) \cap B$. Αρκεί να αποδείξουμε ότι $(A \setminus B) \cap B = \varnothing$. Έστω λοιπόν $x \in (A \setminus B) \cap B \Leftrightarrow (x \in A \setminus B$ και $x \in B) \Leftrightarrow (x \in A$ και $x \notin B$ και $x \in B) \Rightarrow (x \notin B$ και $x \in B)$, αντίφαση. Άρα $(A \setminus B) \cap (A \cap B) = (A \setminus B) \cap B = \varnothing$. Ομοίως $(B \setminus A) \cap (A \cap B) = (B \setminus A) \cap A = \varnothing$. Τώρα, $((A \setminus B) \cup (B \setminus A)) \cap (A \cap B) = ((A \setminus B) \cap (A \cap B)) \cup ((B \setminus A) \cap (A \cap B)) = \varnothing \cup \varnothing = \varnothing$. ■

Σε μια μαθηματική θεωρία συνήθως θεωρούμε ένα **βασικό σύνολο** στο οποίο περιέχονται οι διάφορες έννοιες-στοιχεία και ορισμένα από τα υποσύνολά του (ή και όλα) αποτελούν αντικείμενο μελέτης. Για παράδειγμα, το σύνολο $\mathbb{R}$ των πραγματικών αριθμών ή το σύνολο των συναρτήσεων με πεδίο ορισμού κάποιο υποσύνολο του $\mathbb{R}$ αποτελούν βασικά σύνολα στον Λογισμό μιας Μεταβλητής. Κάθε φορά ορίζουμε το βασικό μας σύνολο και εξετάζουμε τις ιδιότητες των στοιχείων του που ανήκουν σε συγκεκριμένα υποσύνολά του.
Στην απόδειξη των διαφόρων ιδιοτήτων των πράξεων μεταξύ συνόλων (ένωση, τομή, συνολοθεωρητική διαφορά κτλ) σημαντική βοήθεια παρέχουν τα λεγόμενα **διαγράμματα Euler-Venn**. Σ' αυτά το βασικό σύνολο, το οποίο συμβολίζεται συνήθως με Ω, παριστάνεται με ένα ορθογώνιο και τα διάφορα υποσύνολά του με κύκλους, ελλείψεις κτλ, που περιέχονται στο ορθογώνιο αυτό.



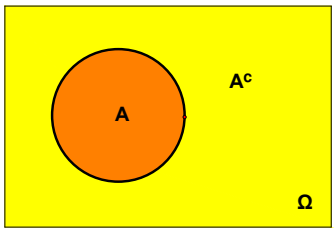
Σχήμα 4

Ορισμός Α΄.12. Έστω Α ένα σύνολο. Τότε με $\mathcal{P}(\mathrm{A})$ συμβολίζουμε **το σύνολο όλων των υποσυνόλων του Α**. Το $\mathcal{P}(\mathrm{A})$ ονομάζεται **δυναμοσύνολο του Α**. Επομένως $\mathcal{P}(\mathrm{A}) = \{\mathrm{X} \mid \mathrm{X} \subseteq \mathrm{A}\}$. Προφανώς $\varnothing \in \mathcal{P}(\mathrm{A})$ και $\mathrm{A} \in \mathcal{P}(\mathrm{A})$.

Συμβολισμός: Το πλήθος των στοιχείων ενός συνόλου Α συμβολίζεται με $\#\mathrm{A}$ ή $|\mathrm{A}|$. Εμείς θα χρησιμοποιήσουμε τον δεύτερο συμβολισμό.
Ας εξετάσουμε την περίπτωση που το Α είναι πεπερασμένο με $n = |\mathrm{A}|$ στοιχεία, όπου $n \geq 0$.
Αν $\mathrm{A} = \varnothing$, δηλαδή $n = 0$, τότε το μόνο υποσύνολο του Α είναι το $\varnothing$. Επομένως $|\mathcal{P}(\mathrm{A})| = 1 = 2^0$.
Αν $n = |\mathrm{A}| = 1$, δηλαδή το Α περιέχει ένα μόνο στοιχείο, π.χ. $\mathrm{A} = \{\alpha\}$, τότε τα μόνα υποσύνολα του Α είναι τα $\varnothing$ και το $\mathrm{A} = \{\alpha\}$. Επομένως $|\mathcal{P}(\mathrm{A})| = 2 = 2^1$.
Αν $n = |\mathrm{A}| = 2$, π.χ. $\mathrm{A} = \{\alpha, \beta\}$, τότε τα υποσύνολα του Α είναι τα $\varnothing$, $\{\alpha\}$, $\{\beta\}$ και το $\mathrm{A} = \{\alpha, \beta\}$. Επομένως $|\mathcal{P}(\mathrm{A})| = 4 = 2^2$.
Από τα προηγούμενα παραδείγματα δημιουργείται η εικασία ότι αν $|\mathrm{A}| = n$, όπου n μη αρνητικός ακέραιος, τότε $|\mathcal{P}(\mathrm{A})| = 2^n$. Σε επόμενο παράρτημα θα αποδείξουμε την εικασία αυτή.

Αν Ω είναι το βασικό μας σύνολο (και όλα τα άλλα σύνολα είναι υποσύνολα αυτού), τότε έχουμε τον ακόλουθο ορισμό:

Ορισμός Α΄.13. Έστω $\mathrm{A} \in \mathcal{P}(\Omega)$. Το **συμπλήρωμα του συνόλου Α** είναι το σύνολο των στοιχείων του Ω που **δεν ανήκουν στο Α**. Το συμπλήρωμα του Α συμβολίζεται με A^c. Δηλαδή, $\mathrm{A}^c = \{x \in \Omega \mid x \notin \mathrm{A}\}$.



Σχήμα 5

Πόρισμα Α΄.14. **(i)** $\mathrm{A}^{cc} := (\mathrm{A}^c)^c = \mathrm{A}$. **(ii)** $\mathrm{A} \cap \mathrm{A}^c = \varnothing$. **(iii)** $\mathrm{A} \cup \mathrm{A}^c = \Omega$. **(iv)** $\mathrm{A} \cap \mathrm{B}^c = \mathrm{A} \setminus \mathrm{B}$.
Απόδειξη: Άσκηση. ■

Πρόταση Α΄.15. (Νόμοι του De Morgan-απλή μορφή) Έστω Α και Β δύο υποσύνολα του βασικού συνόλου Ω. Τότε ισχύουν οι εξής σχέσεις:

(i) $(\mathrm{A} \cup \mathrm{B})^c = \mathrm{A}^c \cap \mathrm{B}^c$ και **(ii)** $(\mathrm{A} \cap \mathrm{B})^c = \mathrm{A}^c \cup \mathrm{B}^c$.

Απόδειξη: **(i)** $x \in (\mathrm{A} \cup \mathrm{B})^c \Leftrightarrow (x \in \Omega$ και $x \notin \mathrm{A} \cup \mathrm{B}) \Leftrightarrow (x \in \Omega$ και $x \notin \mathrm{A}$ και $x \notin \mathrm{B}) \Leftrightarrow ((x \in \Omega$ και $x \notin \notin \mathrm{A})$ και $(x \in \Omega$ και $x \notin \mathrm{B})) \Leftrightarrow (x \in \mathrm{A}^c$ και $x \in \mathrm{B}^c) \Leftrightarrow x \in \mathrm{A}^c \cap \mathrm{B}^c$.
(ii) $x \in (\mathrm{A} \cap \mathrm{B})^c \Leftrightarrow (x \in \Omega$ και $x \notin \mathrm{A} \cap \mathrm{B}) \Leftrightarrow (x \in \Omega$ και $(x \notin \mathrm{A}$ ή $x \notin \mathrm{B})) \Leftrightarrow ((x \in \Omega$ και $x \notin \notin \mathrm{A})$ ή $(x \in \Omega$ και $x \notin \mathrm{B})) \Leftrightarrow (x \in \mathrm{A}^c$ ή $x \in \mathrm{B}^c) \Leftrightarrow x \in \mathrm{A}^c \cup \mathrm{B}^c$. ■

Πρόταση Α΄.16. **(i)** $\mathrm{A} \cup (\mathrm{B} \setminus \mathrm{A}) = \mathrm{A} \cup \mathrm{B}$. **(ii)** $\mathrm{A} \setminus (\mathrm{B} \setminus \Gamma) = (\mathrm{A} \setminus \mathrm{B}) \cup (\mathrm{A} \cap \Gamma)$. **(iii)** $(\mathrm{A} \setminus \mathrm{B}) \setminus \Gamma = \mathrm{A} \setminus (\mathrm{B} \cup \Gamma) = = (\mathrm{A} \setminus \mathrm{B}) \cap (\mathrm{A} \setminus \Gamma)$. **(iv)** $(\mathrm{A} \cup \mathrm{B}) \cap (\Gamma \cup \Delta) = (\mathrm{A} \cap \Gamma) \cup (\mathrm{A} \cap \Delta) \cup (\mathrm{B} \cap \Gamma) \cup (\mathrm{B} \cap \Delta)$.
Απόδειξη: **(i)** $\mathrm{A} \cup (\mathrm{B} \setminus \mathrm{A}) = \mathrm{A} \cup (\mathrm{B} \cap \mathrm{A}^c) = (\mathrm{A} \cup \mathrm{B}) \cap (\mathrm{A} \cup \mathrm{A}^c) = (\mathrm{A} \cup \mathrm{B}) \cap \Omega = \mathrm{A} \cup \mathrm{B}$.
(ii) $\mathrm{A} \setminus (\mathrm{B} \setminus \Gamma) = \mathrm{A} \setminus (\mathrm{B} \cap \Gamma^c) = \mathrm{A} \cap (\mathrm{B} \cap \Gamma^c)^c = \mathrm{A} \cap (\mathrm{B}^c \cup \Gamma) = (\mathrm{A} \cap \mathrm{B}^c) \cup (\mathrm{A} \cap \Gamma) = (\mathrm{A} \setminus \mathrm{B}) \cup (\mathrm{A} \cap \Gamma)$.
(iii) $(\mathrm{A} \setminus \mathrm{B}) \setminus \Gamma = (\mathrm{A} \cap \mathrm{B}^c) \cap \Gamma^c = \mathrm{A} \cap (\mathrm{B}^c \cap \Gamma^c) = \mathrm{A} \cap (\mathrm{B} \cup \Gamma)^c = \mathrm{A} \setminus (\mathrm{B} \cup \Gamma)$. Επίσης, $(\mathrm{A} \setminus \mathrm{B}) \setminus \Gamma = (\mathrm{A} \cap \mathrm{B}^c) \cap \Gamma^c = = (\mathrm{A} \cap \mathrm{B}^c) \cap (\mathrm{A} \cap \Gamma^c) = (\mathrm{A} \setminus \mathrm{B}) \cap (\mathrm{A} \setminus \Gamma)$.
(iv) $(\mathrm{A} \cup \mathrm{B}) \cap (\Gamma \cup \Delta) = (\mathrm{A} \cap (\Gamma \cup \Delta)) \cup (\mathrm{B} \cap (\Gamma \cup \Delta)) = (\mathrm{A} \cap \Gamma) \cup (\mathrm{A} \cap \Delta) \cup (\mathrm{B} \cap \Gamma) \cup (\mathrm{B} \cap \Delta)$. ■

Γνωρίζουμε ότι κάθε σημείο του επιπέδου παριστάνεται, ως προς ένα σύστημα αξόνων, ως ένα **ζεύγος** (α, β) πραγματικών αριθμών. Το α λέγεται τετμημένη και το β τεταγμένη του σημείου. Γενικότερα έχουμε τον ακόλουθο ορισμό:

Ορισμός Α΄.17. Έστω Α και Β δύο σύνολα. Αν $\alpha \in$ Α και $\beta \in$ Β, τότε με το σύμβολο (α, β) παριστάνουμε το **διατεταγμένο ζεύγος** των α και β. Η ισότητα μεταξύ διατεταγμένων ζευγών ορίζεται ως εξής: $(\alpha, \beta) = (\alpha', \beta') \Leftrightarrow (\alpha = \alpha'$ και $\beta = \beta')$, για κάθε $\alpha, \alpha' \in$ Α και $\beta, \beta' \in$ Β.

Υπενθυμίζουμε ότι το διατεταγμένο ζεύγος (α, β) δεν είναι το σύνολο $\{\alpha, \beta\}$. Το ποιο στοιχείο είναι πρώτο και ποιο είναι δεύτερο παίζει ουσιώδη ρόλο. Υπάρχει ένα συνολοθεωρητικό τέχνασμα για να ορίσουμε το διατεταγμένο ζεύγος (α, β), το οποίο οφείλεται στον Kuratowski. Ορίζουμε

$$(\alpha, \beta) = \{\{\alpha\}, \{\alpha, \beta\}\}.$$

Με βάση αυτόν τον ορισμό θα αποδείξουμε ότι: $(\alpha, \beta) = (\gamma, \delta) \Leftrightarrow (\alpha = \gamma$ και $\beta = \delta)$. Διακρίνουμε περιπτώσεις:
α) $\alpha = \beta$. Τότε $(\alpha, \beta) = \{\{\alpha\}, \{\alpha, \alpha\}\} = \{\{\alpha\}, \{\alpha\}\} = \{\{\alpha\}\}$. Εφόσον $(\alpha, \beta) = (\gamma, \delta)$, θα έχουμε $\{\{\alpha\}\} = \{\{\gamma\}, \{\gamma, \delta\}\}$. Εφόσον $\{\gamma, \delta\} \in \{\{\gamma\}, \{\gamma, \delta\}\} = \{\{\alpha\}\}$, παίρνουμε $\{\gamma, \delta\} = \{\alpha\}$. Άρα $\gamma \in \{\alpha\} \Rightarrow \gamma = \alpha$. Ομοίως $\delta = \alpha$. Τελικώς $\alpha = \beta = \gamma = \delta$.
β) $\gamma = \delta$. Εντελώς ανάλογα παίρνουμε πάλι $\alpha = \beta = \gamma = \delta$.
γ) Έστω $\alpha \neq \beta$ και $\gamma \neq \delta$. Από τη σχέση $\{\{\alpha\}, \{\alpha, \beta\}\} = \{\{\gamma\}, \{\gamma, \delta\}\}$ θα έχουμε $\{\alpha\} = \{\gamma\}$ ή $\{\alpha\} = \{\gamma, \delta\}$. Αν $\{\alpha\} = \{\gamma, \delta\}$, τότε $\gamma = \delta = \alpha$, άτοπο από υπόθεση. Άρα $\{\alpha\} = \{\gamma\} \Leftrightarrow \alpha = \gamma$. Επομένως $(\gamma, \delta) = (\alpha, \delta) = \{\{\alpha\}, \{\alpha, \delta\}\}$ και συνεπώς $(\alpha, \beta) = (\gamma, \delta) = (\alpha, \delta) \Leftrightarrow \{\{\alpha\}, \{\alpha, \beta\}\} = \{\{\alpha\}, \{\alpha, \delta\}\}$. Άρα $\{\alpha, \beta\} \in \{\{\alpha\}, \{\alpha, \delta\}\} \Leftrightarrow (\{\alpha, \beta\} = \{\alpha\}$ ή $\{\alpha, \beta\} = \{\alpha, \delta\})$. Αν $\{\alpha, \beta\} = \{\alpha\}$, τότε $\beta = \alpha$, άτοπο από υπόθεση. Άρα $\{\alpha, \beta\} = \{\alpha, \delta\} \Rightarrow \beta \in \{\alpha, \delta\} \underset{\beta \neq \alpha}{\Rightarrow} \beta = \delta$. ■

Ορισμός Α΄.18. Έστω Α, Β δύο σύνολα. Το σύνολο $\text{Α} \times \text{Β} = \{(\alpha, \beta) \mid \alpha \in \text{Α}$ και $\beta \in \text{Β}\}$ ονομάζεται **καρτεσιανό γινόμενο του Α επί το Β**.

Πρόταση Α΄.19. Ισχύουν τα ακόλουθα: **(i)** $\text{Α} \times \text{Β} = \varnothing \Leftrightarrow (\text{Α} = \varnothing$ ή $\text{Β} = \varnothing)$.
(ii) $\text{Α} \times (\text{Β} \setminus \Gamma) = (\text{Α} \times \text{Β}) \setminus (\text{Α} \times \Gamma)$. **(iii)** $(\text{Α} \setminus \Gamma) \times \text{Β} = (\text{Α} \times \text{Β}) \setminus (\Gamma \times \text{Β})$.
Απόδειξη: (i) Έστω $\text{Α} \times \text{Β} = \varnothing$. Υποθέτουμε ότι $\text{Α} \neq \varnothing$ και $\text{Β} \neq \varnothing$. Τότε υπάρχει $\alpha \in$ Α και $\beta \in$ Β. Αλλά τότε $(\alpha, \beta) \in \text{Α} \times \text{Β} \Rightarrow \text{Α} \times \text{Β} \neq \varnothing$, άτοπο. Αντιστρόφως, έστω Α$= \varnothing$. Αν $\text{Α} \times \text{Β} \neq \varnothing$, τότε θα υπήρχαν $\alpha \in$ Α και $\beta \in$ Β, ώστε $(\alpha, \beta) \in \text{Α} \times \text{Β}$. Αλλά από τη σχέση $\alpha \in$ Α προκύπτει ότι $\text{Α} \neq \varnothing$, άτοπο. Άρα $\text{Α} \times \text{Β} = \varnothing$. Παρόμοια προκύπτει ότι αν $\text{Β} = \varnothing$, τότε $\text{Α} \times \text{Β} = \varnothing$.
(ii) $(\alpha, \beta) \in \text{Α} \times (\text{Β} \setminus \Gamma) \Leftrightarrow (\alpha \in$ Α και $\beta \in \text{Β} \setminus \Gamma) \Leftrightarrow (\alpha \in$ Α και $\beta \in$ Β και $\beta \notin \Gamma) \Leftrightarrow ((\alpha, \beta) \in \in \text{Α} \times \text{Β}$ και $(\alpha, \beta) \notin \text{Α} \times \Gamma) \Leftrightarrow (\alpha, \beta) \in (\text{Α} \times \text{Β}) \setminus (\text{Α} \times \Gamma)$.
(iii) Η απόδειξη είναι παρόμοια με την προηγούμενη. ■

Ορισμός Α΄.20. Αν Α και Β είναι δύο μη κενά σύνολα, τότε ένα υποσύνολο σ του $\text{Α} \times \text{Β}$ λέμε ότι ορίζει μια **διμελή σχέση μεταξύ των Α και Β**. Ακριβέστερα, μια διμελής σχέση σ μεταξύ των Α και Β είναι ένα υποσύνολο του $\mathcal{P}(\text{Α} \times \text{Β})$ της μορφής $\{\text{Α} \times \text{Β}, \text{G}_\sigma\}$, όπου $\text{G}_\sigma \subseteq \text{Α} \times \text{Β}$. Το $\text{G}_\sigma \subseteq \text{Α} \times \text{Β}$ λέγεται **γράφημα** της σχέσης σ. Ενδιαφέρον υπάρχει όταν το G_σ είναι μη κενό.

Ορισμός Α΄.21. (i) Αν Α και Β είναι δύο σύνολα, τότε μια διμελής σχέση $f = \{\text{Α} \times \text{Β}, \text{G}_f\}$ θα λέγεται **συνάρτηση (ή απεικόνιση) από το Α στο Β** και θα γράφουμε $f : \text{Α} \to \text{Β}$, αν ισχύει το εξής: Για κάθε $x \in$ Α υπάρχει **μοναδικό** $y \in$ Β τέτοιο, ώστε $(x, y) \in \text{G}_f$. Δηλαδή, αν $(x, y) \in \text{G}_f$ και $(x, y') \in \text{G}_f$, τότε $y = y'$. Η σχέση $(x, y) \in \text{G}_f$ γράφεται ισοδύναμα ως εξής: $f(x) = y$ ή $x \overset{f}{\mapsto} y$. Το $y = f(x)$ λέγεται **εικόνα ή τιμή** του x μέσω της συνάρτησης f.
(ii) Το σύνολο Α λέγεται **πεδίο ορισμού** της συνάρτησης.
(iii) Το σύνολο Β λέγεται **πεδίο τιμών** της συνάρτησης.
(iv) Το σύνολο $\{f(x) \mid x \in \text{Α}\} \subseteq \text{Β}$ λέγεται **σύνολο τιμών της f**. Αυτό παριστάνεται με $f(\text{Α})$. Αν $f(\text{Α}) = \text{Β}$, τότε η συνάρτηση f λέγεται **επί**. (surjection)
(v) Αν για κάθε $x, x' \in$ Α, με $x \neq x'$ ισχύει $f(x) \neq f(x')$, τότε η f λέγεται **ένα προς ένα (1-1)**. (injection) Η προηγούμενη συνθήκη είναι ισοδύναμη με την: Αν $x, x' \in$ Α με $f(x) = f(x')$, τότε $x = x'$.
(vi) Αν μια συνάρτηση $f : \text{Α} \to \text{Β}$ είναι 1-1 και επί, τότε λέγεται **αμφιμονοσήμαντη αντιστοιχία**. (bijection).

Σχόλιο: Για κάποιον περίεργο λόγο στα σχολικά βιβλία όλες οι συναρτήσεις θεωρούνται επί! Προφανώς λόγω κάποιας «απλούστευσης» (η οποία δεν είναι επιστημονικώς ορθή και δημιουργεί μετέπειτα σύγχυση, οι συγγραφείς των βιβλίων αυτών ταυτίζουν το σύνολο Β με το σύνολο τιμών $f(\mathrm{A})$). Για παράδειγμα, η συνάρτηση $f:\mathbb{R}\to\mathbb{R}$ με $f(x)=x^2$, για κάθε $x\in\mathbb{R}$ **δεν είναι επί**. Η συνάρτηση όμως $g:\mathbb{R}\to[0,+\infty)$ με $g(x)=x^2$, για κάθε $x\in\mathbb{R}$ είναι επί. Δεν πρέπει να ξεχνάμε ότι μια συνάρτηση f ορίζεται από δύο ή ουσιαστικά τρία πράγματα: Το σύνολο $\mathrm{A}\times\mathrm{B}$, το οποίο καθορίζει το πεδίο ορισμού Α και το σύνολο Β, **(το Β περιέχει το σύνολο τιμών)** και το γράφημα $\mathrm{G}_f\subseteq\mathrm{A}\times\mathrm{B}$.

Ορισμός Α΄.22. Αν $f:\mathrm{A}\to\mathrm{B}$ και $g:\mathrm{B}\to\Gamma$ είναι δύο συναρτήσεις, τότε ορίζεται η συνάρτηση $g\circ f:\mathrm{A}\to\Gamma$ με γράφημα $\{(x,g(f(x)))\mid x\in\mathrm{A}\}\subseteq\mathrm{A}\times\Gamma$, δηλαδή $(g\circ f)(x)=g(f(x))$, για κάθε $x\in\mathrm{A}$. Η $g\circ f$ διαβάζεται ***g* σύνθεση *f***. Επομένως $(x,z)\in\mathrm{G}_{g\circ f}\Leftrightarrow$ (υπάρχει (μοναδικό) $y\in\mathrm{B}$ τέτοιο, ώστε $(x,y)\in\mathrm{G}_f$ και $(y,z)\in\in\mathrm{G}_g$).

Πρόταση Α΄.23. Αν $f:\mathrm{A}\to\mathrm{B}$, $g:\mathrm{B}\to\Gamma$ και $h:\Gamma\to\Delta$, τότε $(h\circ g)\circ f=h\circ(g\circ f):A\to\Delta$.
Απόδειξη: Έστω $x\in\mathrm{A}$. Τότε έχουμε: $((h\circ g)\circ f)(x)=(h\circ g)(f(x))=h(g(f(x)))=h((g\circ f)(x))=$ $=(h\circ(g\circ f))(x)$. ■

Έστω $f:\mathrm{A}\to\mathrm{B}$ μια 1-1 και επί απεικόνιση. Ορίζουμε τη σχέση f^{-1} μεταξύ των Β και Α με γράφημα $\mathrm{G}_{f^{-1}}=\{(y,x)\mid(x,y)\in\mathrm{G}_f\}$. Η f^{-1} είναι μια απεικόνιση από το Β στο Α, η οποία είναι επίσης 1-1 και επί. Πράγματι, αν $y\in\mathrm{B}$, τότε επειδή η f είναι επί, υπάρχει $x\in\mathrm{A}$ τέτοιο, ώστε $y=f(x)\Leftrightarrow(x,y)\in\in\mathrm{G}_f\Leftrightarrow(y,x)\in\mathrm{G}_{f^{-1}}$. Επειδή η f είναι 1-1, το $x\in\mathrm{A}$ είναι μοναδικό. Άρα, για κάθε $y\in\mathrm{B}$ υπάρχει μοναδικό $x\in\mathrm{A}$ τέτοιο, ώστε $(y,x)\in\mathrm{G}_{f^{-1}}$. Άρα ορίζεται μια συνάρτηση $f^{-1}:\mathrm{B}\to\mathrm{A}$ μέσω της ισοδυναμίας: $y=f(x)\Leftrightarrow x=f^{-1}(y)$. Η συνάρτηση f^{-1} είναι 1-1. Πράγματι, έστω $f^{-1}(y)=f^{-1}(y')=x$. Τότε $(y,x)\in\mathrm{G}_{f^{-1}}\Leftrightarrow(x,y)\in\mathrm{G}_f$ και $(y',x)\in\mathrm{G}_{f^{-1}}\Leftrightarrow(x,y')\in\mathrm{G}_f$, δηλαδή $y=f(x)=y'$. Τέλος, η $f^{-1}:\mathrm{B}\to\mathrm{A}$ είναι επί. Πράγματι, αν $x\in\mathrm{A}$ και $y=f(x)$, τότε $x=f^{-1}(y)$, από τον ορισμό της f^{-1}.

Ορισμός Α΄.24. Αν $f:\mathrm{A}\to\mathrm{B}$ είναι 1-1 και επί, η συνάρτηση $f^{-1}:\mathrm{B}\to\mathrm{A}$ που ορίσαμε προηγουμένως λέγεται **αντίστροφη της *f***.

Ορισμός Α΄.25. Αν $\mathrm{A}\neq\varnothing$, η συνάρτηση $1_\mathrm{A}:\mathrm{A}\to\mathrm{A}$ με γράφημα τη **διαγώνιο** $\{(x,x)\mid\ x\in\mathrm{A}\}$ του Α, δηλαδή $1_\mathrm{A}(x)=x$, για κάθε $x\in\mathrm{A}$, λέγεται **η ταυτοτική συνάρτηση του Α**.

Πρόταση Α΄.26. Έστω $f:\mathrm{A}\to\mathrm{B}$ μια 1-1 και επί συνάρτηση. Τότε ισχύουν οι σχέσεις: $f^{-1}\circ f=1_\mathrm{A}$ και $f\circ f^{-1}=1_\mathrm{B}$.
Απόδειξη: Έστω $x\in\mathrm{A}$ και $y=f(x)\in\mathrm{B}$. Τότε $f^{-1}(y)=x$. Άρα $(f^{-1}\circ f)(x)=f^{-1}(f(x))=f^{-1}(y)=$ $=x$. Αντιστρόφως, έστω $y\in\mathrm{B}$ και $x=f^{-1}(y)\in\mathrm{A}$. Τότε $f(x)=y$. Άρα $(f\circ f^{-1})(y)=f(f^{-1}(y))=f(x)=$ $=y$. ■

Ορισμός Α΄.27. Έστω $f:\mathrm{A}\to\mathrm{B}$.
(i) Αν $\mathrm{X}\subseteq\mathrm{A}$, τότε το σύνολο $f(\mathrm{X})=\{f(x)\mid x\in\mathrm{X}\}\subseteq\mathrm{B}$ ονομάζεται **εικόνα** του Χ μέσω της f.
(ii) Αν $\mathrm{Y}\subseteq\mathrm{B}$, τότε το σύνολο $f^{-1}(\mathrm{Y})=\{x\in\mathrm{A}\mid f(x)\in\mathrm{Y}\}\subseteq\mathrm{A}$ ονομάζεται **αντίστροφη εικόνα** του Υ μέσω της f.

Πρόταση Α΄.28. Έστω $f:\mathrm{A}\to\mathrm{B}$. Τότε ισχύουν τα ακόλουθα:
(i) $f(\varnothing)=\varnothing$ και $f^{-1}(\varnothing)=\varnothing$.
(ii) Αν $\mathrm{X},\ \mathrm{X}'\subseteq\mathrm{A}$, τότε $f(\mathrm{X}\cup\mathrm{X}')=f(\mathrm{X})\cup f(\mathrm{X}')$ και $f(\mathrm{X}\cap\mathrm{X}')\subseteq f(\mathrm{X})\cap f(\mathrm{X}')$.
(iii) Αν $\mathrm{Y},\ \mathrm{Y}'\subseteq\mathrm{B}$, τότε $f^{-1}(\mathrm{Y}\cup\mathrm{Y}')=f^{-1}(\mathrm{Y})\cup f^{-1}(\mathrm{Y}')$ και $f^{-1}(\mathrm{Y}\cap\mathrm{Y}')=f^{-1}(\mathrm{Y})\cap f^{-1}(\mathrm{Y}')$.
Απόδειξη: (i) Έστω $f(\varnothing)\neq\varnothing$ και άρα υπάρχει $y\in f(\varnothing)$. Τότε υπάρχει $x\in\varnothing$ με $y=f(x)$, άτοπο. Αν $f^{-1}(\varnothing)\neq\varnothing$ και $x\in f^{-1}(\varnothing)$, τότε $f(x)\in\varnothing$, άτοπο.
(ii) Έστω $x\in\mathrm{X}\cup\mathrm{X}'$. Τότε $x\in\mathrm{X}$ ή $x\in\mathrm{X}'$. Αν $x\in\mathrm{X}$, τότε $f(x)\in f(\mathrm{X})\subseteq f(\mathrm{X})\cup f(\mathrm{X}')$. Ομοίως, αν $x\in\mathrm{X}'$, τότε $f(x)\in f(\mathrm{X})\cup f(\mathrm{X}')$. Άρα $f(\mathrm{X}\cup\mathrm{X}')\subseteq f(\mathrm{X})\cup f(\mathrm{X}')$. Αντιστρόφως, έστω $y\in f(\mathrm{X})\cup f(\mathrm{X}')$. Τότε $y\in f(\mathrm{X})$ ή $y\in f(\mathrm{X}')$. Αν $y\in f(\mathrm{X})$, τότε υπάρχει $x\in\mathrm{X}\subseteq\mathrm{X}\cup\mathrm{X}'$ τέτοιο, ώστε $y=f(x)$. Άρα $y\in f(\mathrm{X}\cup\mathrm{X}')$. Ομοίως, αν $y\in f(\mathrm{X}')$, τότε $y\in f(\mathrm{X}\cup\mathrm{X}')$. Επομένως $f(\mathrm{X}\cup\mathrm{X}')=f(\mathrm{X})\cup f(\mathrm{X}')$.

Προφανώς, αν $\mathrm{T} \subseteq \mathrm{S} \subseteq \mathrm{A}$, τότε $f(\mathrm{T}) \subseteq f(\mathrm{S})$. Επομένως, $\mathrm{X} \cap \mathrm{X}' \subseteq \mathrm{X} \Rightarrow f(\mathrm{X} \cap \mathrm{X}') \subseteq f(\mathrm{X})$. Ομοίως, $\mathrm{X} \cap \mathrm{X}' \subseteq \mathrm{X}' \Rightarrow f(\mathrm{X} \cap \mathrm{X}') \subseteq f(\mathrm{X}')$. Επομένως $f(\mathrm{X} \cap \mathrm{X}') \subseteq f(\mathrm{X}) \cap f(\mathrm{X}')$. Ισότητα εν γένει δεν ισχύει στην περίπτωση αυτή, όπως φαίνεται στο ακόλουθο παράδειγμα: $f : \mathbb{R} \to [0, +\infty)$ με $f(x) = x^2$, για κάθε $x \in \mathbb{R}$. Έστω $\mathrm{X} = \{-1\}$ και $\mathrm{X}' = \{1\}$. Τότε $\mathrm{X} \cap \mathrm{X}' = \varnothing$ και συνεπώς $f(\mathrm{X} \cap \mathrm{X}') = \varnothing$. Αλλά $f(\mathrm{X}) = f(\mathrm{X}') = \{1\}$.
(iii) $x \in f^{-1}(\mathrm{Y} \cup \mathrm{Y}') \Leftrightarrow f(x) \in \mathrm{Y} \cup \mathrm{Y}' \Leftrightarrow (f(x) \in \mathrm{Y}$ ή $f(x) \in \mathrm{Y}') \Leftrightarrow (x \in f^{-1}(\mathrm{Y})$ ή $x \in f^{-1}(\mathrm{Y}')) \Leftrightarrow x \in$ $\in f^{-1}(\mathrm{Y}) \cup f^{-1}(\mathrm{Y}')$.
$x \in f^{-1}(\mathrm{Y} \cap \mathrm{Y}') \Leftrightarrow f(x) \in \mathrm{Y} \cap \mathrm{Y}' \Leftrightarrow (f(x) \in \mathrm{Y}$ και $f(x) \in \mathrm{Y}') \Leftrightarrow (x \in f^{-1}(\mathrm{Y})$ και $x \in f^{-1}(\mathrm{Y}')) \Leftrightarrow x \in$ $\in f^{-1}(\mathrm{Y}) \cap f^{-1}(\mathrm{Y}')$. ■

Ορισμός Α΄.29. Μια ακολουθία στοιχείων ενός συνόλου Α είναι μια απεικόνιση $\alpha : \mathbb{N} \to \mathrm{X}$ ή $\alpha : \mathbb{Z}_+ \to \mathrm{X}$, όπου $\mathbb{N}$ και $\mathbb{Z}_+$ τα σύνολα των φυσικών και θετικών ακεραίων, αντίστοιχα. Στις ακολουθίες συνήθως γράφουμε α_n αντί $\alpha(n)$. Μια **πεπερασμένη** ακολουθία έχει πεδίο ορισμού το σύνολο $\{0, 1, 2, \ldots, n\}$ ή το $\{1, 2, \ldots, n\}$. (Το σύνολα των φυσικών και των ακεραίων ορίζονται στο επόμενο παράρτημα). Γενικότερα, αν Ι είναι ένα **σύνολο δεικτών**, μια **οικογένεια** με δείκτες από το Ι είναι μια απεικόνιση $\alpha : \mathrm{I} \to \mathrm{X}$. Συνήθως μια οικογένεια παριστάνεται με το σύμβολο $(\alpha_i)_{i \in \mathrm{I}}$.
Ας υποθέσουμε ότι $\mathcal{A}$ είναι ένα μη κενό σύνολο υποσυνόλων ενός βασικού συνόλου Ω, δηλαδή $\mathcal{A} \subseteq \mathcal{P}(\Omega)$. (Για ένα σύνολο συνόλων προτιμούμε τον όρο «συλλογή»). Αν υπάρχει ανάγκη «παραμετρικοποίησης» των στοιχείων-συνόλων της συλλογής με βάση ένα σύνολο δεικτών Ι, δηλαδή αν θέλουμε να διαφοροποιήσουμε τα στοιχεία του $\mathcal{A}$ με βάση κάποιους δείκτες από ένα σύνολο Ι, θεωρούμε την $\mathcal{A}$ ως σύνολο εικόνων μιας οικογένειας και γράφουμε $\mathcal{A} = \{\mathrm{A}_i \mid i \in \mathrm{I}\}$. Λόχου χάριν, αν η $\mathcal{A}$ είναι πεπερασμένη, γράφουμε $\mathcal{A} = \{\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n\} = \{\mathrm{A}_i \mid i = 1, 2, \ldots, n\}$. Αυτό μπορεί να συμβεί και όταν το σύνολο δεικτών δεν είναι υποσύνολο του $\mathbb{N}$. Αν δεν υπάρχει τέτοια ανάγκη ιδιαίτερου συμβολισμού, γράφουμε $\mathrm{A} \in \mathcal{A}$ ή (τετριμμένα) $\mathcal{A} = \{\mathrm{A} \mid \mathrm{A} \in \mathcal{A}\}$. Στην τελευταία περίπτωση έχουμε θεωρήσει το $\mathcal{A}$ σαν το σύνολο των εικόνων της ταυτοτικής οικογένειας $1_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}$ με σύνολο δεικτών το ίδιο το $\mathcal{A}$.

Ορισμός Α΄.30. Έστω $\mathcal{A}$ μια μη κενή συλλογή, οικογένεια (όπως θέλετε πείτε τη) υποσυνόλων ενός βασικού συνόλου Ω.
(i) Ορίζουμε την **ένωση $\bigcup_{\mathrm{A} \in \mathcal{A}} \mathrm{A}$ των συνόλων της συλλογής $\mathcal{A}$** ως το σύνολο των στοιχείων x, τα οποία ανήκουν **σε κάποιο** $\mathrm{A} \in \mathcal{A}$. Δηλαδή $\bigcup_{\mathrm{A} \in \mathcal{A}} \mathrm{A} = \{x \mid x \in \mathrm{A}$, για κάποιο $\mathrm{A} \in \mathcal{A}\}$. Πολλές φορές γράφουμε απλώς $\bigcup \mathcal{A}$ αντί $\bigcup_{\mathrm{A} \in \mathcal{A}} \mathrm{A}$. Αν η συλλογή $\mathcal{A}$ είναι πεπερασμένη, ήτοι $\mathcal{A} = \{\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n\}$, μπορούμε να γράψουμε την ένωση αυτή ως $\mathrm{A}_1 \cup \mathrm{A}_2 \cup \cdots \cup \mathrm{A}_n$ ή $\bigcup_{i=1}^{n} \mathrm{A}_i$.
(ii) Ορίζουμε την **τομή $\bigcap_{\mathrm{A} \in \mathcal{A}} \mathrm{A}$ των συνόλων της συλλογής $\mathcal{A}$** ως το σύνολο των στοιχείων x, τα οποία ανήκουν **σε κάθε** $\mathrm{A} \in \mathcal{A}$. Δηλαδή $\bigcap_{\mathrm{A} \in \mathcal{A}} \mathrm{A} = \{x \mid x \in \mathrm{A}$, για κάθε $\mathrm{A} \in \mathcal{A}\}$. Πολλές φορές γράφουμε απλώς $\bigcap \mathcal{A}$ αντί $\bigcap_{\mathrm{A} \in \mathcal{A}} \mathrm{A}$. Αν η συλλογή $\mathcal{A}$ είναι πεπερασμένη, ήτοι $\mathcal{A} = \{\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n\}$, μπορούμε να γράψουμε την τομή αυτή ως $\mathrm{A}_1 \cap \mathrm{A}_2 \cap \cdots \cap \mathrm{A}_n$ ή $\bigcap_{i=1}^{n} \mathrm{A}_i$.

Πρόταση Α΄.31. (Νόμοι του De Morgan-Γενική μορφή) Έστω $\mathcal{A}$ μια μη κενή συλλογή υποσυνόλων ενός βασικού συνόλου Ω, δηλαδή $\varnothing \neq \mathcal{A} \subseteq \mathcal{P}(\Omega)$. Τότε ισχύουν τα εξής:

(i) $$\left(\bigcup_{\mathrm{A} \in \mathcal{A}} \mathrm{A}\right)^c = \bigcap_{\mathrm{A} \in \mathcal{A}} \mathrm{A}^c$$

(ii) $$\left(\bigcap_{\mathrm{A} \in \mathcal{A}} \mathrm{A}\right)^c = \bigcup_{\mathrm{A} \in \mathcal{A}} \mathrm{A}^c$$

Απόδειξη: (i) Έστω $\alpha \in \Omega$. Τότε $\alpha \in \left(\bigcup_{\mathrm{A} \in \mathcal{A}} \mathrm{A}\right)^c \Leftrightarrow \alpha \notin \bigcup_{\mathrm{A} \in \mathcal{A}} \mathrm{A} = \{x \in \Omega \mid x \in \mathrm{A}$, για κάποιο $\mathrm{A} \in \mathcal{A}\} \Leftrightarrow (x \notin$ $\notin \mathrm{A}$, για κάθε $\mathrm{A} \in \mathcal{A}) \Leftrightarrow (x \in \mathrm{A}^c$, για κάθε $\mathrm{A} \in \mathcal{A}) \Leftrightarrow x \in \bigcap_{\mathrm{A} \in \mathcal{A}} \mathrm{A}^c$.

(ii) Έστω $\alpha \in \Omega$. Τότε $\alpha \in \left(\bigcap_{A\in\mathcal{A}} A\right)^c \Leftrightarrow \alpha \notin \bigcap_{A\in\mathcal{A}} A = \{x \in \Omega \mid x \in A, \text{ για κάθε } A \in \mathcal{A}\} \Leftrightarrow (x \notin$ $\notin A$, για κάποιο $A \in \mathcal{A}) \Leftrightarrow (x \in A^c$, για κάποιο $A \in \mathcal{A}) \Leftrightarrow x \in \bigcup_{A\in\mathcal{A}} A^c$. ■

Προσέξτε ότι στα δεύτερα μέλη των σχέσεων **(i)** και **(ii)** δεν εμφανίζονται ενώσεις ή τομές στοιχείων της συλλογής $\mathcal{A}$. Πρόκειται για ενώσεις ή τομές στοιχείων μιας οικογένειας με σύνολο δεικτών την $\mathcal{A}$. Το ίδιο συμβαίνει και στις ακόλουθες προτάσεις:

Πρόταση Α΄.32. Έστω $\mathcal{A}$ όπως παραπάνω και $B \subseteq \Omega$. Τότε ισχύουν τα εξής:
(i) $\left(\bigcup_{A\in\mathcal{A}} A\right) \cap B = \bigcup_{A\in\mathcal{A}} (A \cap B)$ και
(ii) $\left(\bigcap_{A\in\mathcal{A}} A\right) \cup B = \bigcap_{A\in\mathcal{A}} (A \cup B)$.

Απόδειξη: (i) $x \in \left(\bigcup_{A\in\mathcal{A}} A\right) \cap B \Leftrightarrow (x \in \bigcup_{A\in\mathcal{A}} A$ και $x \in B) \Leftrightarrow (x \in A$, για κάποιο $A \in \mathcal{A}$ και $x \in B) \Leftrightarrow (x \in$ $\in A \cap B$, για κάποιο $A \in \mathcal{A}) \Leftrightarrow x \in \bigcup_{A\in\mathcal{A}} (A \cap B)$.

(ii) $x \in \left(\bigcap_{A\in\mathcal{A}} A\right) \cup B \Leftrightarrow (x \in \bigcap_{A\in\mathcal{A}} A$ ή $x \in B) \Leftrightarrow (x \in A$, για κάθε $A \in \mathcal{A}$ ή $x \in B) \Leftrightarrow (x \in A \cup$ $\cup B$, για κάθε $A \in \mathcal{A}) \Leftrightarrow x \in \bigcap_{A\in\mathcal{A}} (A \cup B)$. ■

Πρόταση Α΄.33. (i) Αν $\mathcal{A}$ είναι μια συλλογή συνόλων, τότε ισχύουν οι σχέσεις: $\left(\bigcup_{A\in\mathcal{A}} A\right) \times B = \bigcup_{A\in\mathcal{A}} (A \times B)$ και $\left(\bigcap_{A\in\mathcal{A}} A\right) \times B = \bigcap_{A\in\mathcal{A}} (A \times B)$.

(ii) Αν $\mathcal{B}$ είναι μια συλλογή συνόλων, τότε ισχύουν οι σχέσεις: $A \times \left(\bigcup_{B\in\mathcal{B}} B\right) = \bigcup_{B\in\mathcal{B}} (A \times B)$ και $A \times \left(\bigcap_{B\in\mathcal{B}} B\right) =$ $= \bigcap_{B\in\mathcal{B}} (A \times B)$.

Απόδειξη: (i) $(\alpha, \beta) \in \left(\bigcup_{A\in\mathcal{A}} A\right) \times B \Leftrightarrow (\alpha \in \bigcup_{A\in\mathcal{A}} A$ και $\beta \in B) \Leftrightarrow (\alpha \in A$, για κάποιο $A \in \mathcal{A}$ και $\beta \in B) \Leftrightarrow$ $((\alpha, \beta) \in \in A \times B$, για κάποιο $A \in \mathcal{A}) \Leftrightarrow (\alpha, \beta) \in \bigcup_{A\in\mathcal{A}} (A \times B)$.

Επίσης, $(\alpha, \beta) \in \left(\bigcap_{A\in\mathcal{A}} A\right) \times B \Leftrightarrow (\alpha \in \bigcap_{A\in\mathcal{A}} A$ και $\beta \in B) \Leftrightarrow (\alpha \in A$, για κάθε $A \in \mathcal{A}$ και $\beta \in B) \Leftrightarrow ((\alpha, \beta) \in$ $\in A \times B$, για κάθε $A \in \mathcal{A}) \Leftrightarrow (\alpha, \beta) \in \bigcap_{A\in\mathcal{A}} (A \times B)$.
(ii) Παρόμοια με την προηγούμενη. ■

Ορισμός Α΄.34. Έστω $\sigma = \{A \times A, G_\sigma\}$ μια διμελής σχέση, όπου $A \neq \varnothing$. Αυτή λέγεται **μια διμελής σχέση στο Α**. Αντί $(x, y) \in G_\sigma$, θα γράφουμε $x\sigma y$.
(i) Μια σχέση σ στο Α λέγεται **αυτοπαθής** ή **ανακλαστική**, αν και μόνον αν $x\sigma x$, για κάθε $x \in A$.
(ii) Μια σχέση σ στο Α λέγεται **συμμετρική**, αν και μόνον αν, για κάθε $x, y \in A$ ισχύει η ισοδυναμία: $x\sigma y \Leftrightarrow y\sigma x$.
(iii) Μια σχέση σ στο Α λέγεται **αντισυμμετρική**, αν και μόνον αν, για κάθε $x, y \in A$ ισχύει η συνεπαγωγή: $(x\sigma y$ και $y\sigma x) \Rightarrow x = y$.
(iv) Μια σχέση σ στο Α λέγεται **μεταβατική**, αν και μόνον αν, για κάθε $x, y, z \in A$ ισχύει η συνεπαγωγή: $(x\sigma y$ και $y\sigma z) \Rightarrow x\sigma z$.

Ορισμός Α΄.35. Έστω σ μια (διμελής) σχέση στο $A \neq \varnothing$. Η σ λέγεται **σχέση μερικής διάταξης** ή **μερική διάταξη του Α** και το Α **μερικώς διατεταγμένο σύνολο**, αν η σ είναι:
(i) Ανακλαστική, **(ii)** αντισυμμετρική και **(iii)** μεταβατική.

Συνήθως αντί του σ χρησιμοποιούμε κάποιο από τα σύμβολα $\leq, \preceq, \subseteq, \sqsubseteq, \leqslant, \lesssim, \precsim$ κτλ. Μια μερική διάταξη $\preceq$ λέγεται **ολική** ή **γραμμική** αν κάθε δύο στοιχεία του A είναι συγκρίσιμα, δηλαδή, για κάθε $x, y \in \mathrm{A}$ έχουμε $x \preceq y$ ή $y \preceq x$.

Παραδείγματα: 1) Έστω Ω ένα βασικό σύνολο και $\mathrm{A} = \mathcal{P}(\Omega)$. Η σχέση $\subseteq$ του «περιέχεσθαι» είναι μια μερική διάταξη στο A. Αν το Ω περιέχει δύο τουλάχιστον στοιχεία α και β, η σχέση αυτή δεν είναι γραμμική διάταξη. (Γιατί τα σύνολα $\{\alpha\}$ και $\{\beta\}$ δεν είναι συγκρίσιμα). Αν όμως $\mathrm{A} = \{\varnothing, \{0\}, \{0,1\}, \{0,1,2\}\}$, η σχέση $\subseteq$ είναι γραμμική στο A.
2) Η σχέση $\leq$ είναι γραμμική διάταξη σε κάθε μη κενό υποσύνολο A του $\mathbb{R}$.
3) Έστω A το σύνολο των κύκλων του επιπέδου με το ίδιο κέντρο O. Αν $C_1, C_2 \in \mathrm{A}$ μπορούμε να γράψουμε $C_1 \preceq C_2$ αν και μόνον αν η ακτίνα του C_1 είναι μικρότερη ή ίση της ακτίνας του C_2. Η $\preceq$ είναι μια γραμμική διάταξη στο A.
4) Έστω V ένας διανυσματικός χώρος επί του $\mathbb{R}$ ή του $\mathbb{C}$. Αν X είναι το σύνολο των διανυσματικών υπόχωρων του V, τότε η σχέση $\leqslant$ μεταξύ των υπόχωρων είναι μια σχέση διάταξης στο X.

Ορισμός Α΄.36. Έστω σ μια (διμελής) σχέση στο $\mathrm{A} \neq \varnothing$. Η σ λέγεται **σχέση ισοδυναμίας** ή απλά **ισοδυναμία** στο A, αν η σ είναι:
(i) Ανακλαστική, **(ii)** συμμετρική και **(iii)** μεταβατική.
Εδώ αντί του σ, χρησιμοποιούμε κάποιο από τα σύμβολα $\sim, \simeq, \equiv$ κτλ.

Παραδείγματα: 1) Η **ισότητα** των στοιχείων ενός μη κενού συνόλου A είναι σχέση ισοδυναμίας.
2) Στη Γεωμετρία έχουμε μάθει ότι δύο κύκλοι είναι ίσοι αν και μόνον αν έχουν ίσες ακτίνες. Επειδή δύο τέτοιοι κύκλοι εν γένει ως σύνολα δεν ταυτίζονται, αφού ενδεχομένως περιέχουν διαφορετικά σημεία, είναι προτιμότερο να θεωρούνται **ισοδύναμοι**. Η σχέση λοιπόν $C_1 \equiv C_2$ αν και μόνον αν οι κύκλοι C_1 και C_2 έχουν ίσες ακτίνες, είναι σχέση ισοδυναμίας.
3) Στο σύνολο των κύκλων του επιπέδου ορίζουμε τη σχέση $\sim$ με $C_1 \sim C_2$ αν και μόνον αν οι κύκλοι C_1 και C_2 είναι ομόκεντροι. Η σχέση $\sim$ είναι σχέση ισοδυναμίας.
4) Δύο ευθείες $\varepsilon_1, \varepsilon_2$ του επιπέδου (ή του χώρου) θα λέγονται ισοδύναμες αν και μόνον αν ταυτίζονται ή είναι παράλληλες. Μπορούμε να γράφουμε $\varepsilon_1 // \varepsilon_2$. Η σχέση // είναι σχέση ισοδυναμίας στο σύνολο των ευθειών του χώρου.
5) Στο σύνολο $\mathbb{R}$ των πραγματικών ορίζουμε την εξής σχέση: $x \sim y \Leftrightarrow x - y \in \mathbb{Q}$. Η $\sim$ είναι σχέση ισοδυναμίας. Πράγματι, $x - x = 0 \in \mathbb{Q} \Leftrightarrow x \sim x$, για κάθε $x \in \mathbb{R}$. (Ανακλαστική), $x \sim y \Leftrightarrow x - y \in \mathbb{Q} \Leftrightarrow y - x = -(x - y) \in \mathbb{Q} \Leftrightarrow y \sim x$ (Συμμετρική) και αν $x \sim y$ και $y \sim z$, τότε $x - y \in \mathbb{Q}$ και $y - z \in \mathbb{Q}$ και συνεπώς $x - z = (x - y) + (y - z) \in \mathbb{Q} \Leftrightarrow x \sim z$ (Μεταβατική).
6) Έστω V διανυσματικός χώρος επί ενός σώματος $\mathbb{F}$ και $\mathrm{W} \leqslant \mathrm{V}$. Ορίζουμε μια σχέση $\sim$ στο V ως εξής: $v \sim u \Leftrightarrow v - u \in \mathrm{W}$. Η $\sim$ είναι σχέση ισοδυναμίας στο V. Η απόδειξη είναι παρόμοια με την προηγούμενη. Σημειώνουμε μάλιστα ότι το προηγούμενο παράδειγμα είναι ειδική περίπτωση αυτού του παραδείγματος, αφού το $\mathbb{Q}$ είναι μονοδιάστατος διανυσματικός χώρος επί του εαυτού του και το $\mathbb{R}$ απειροδιάστατος διανυσματικός χώρος επί του $\mathbb{Q}$, ο οποίος προφανώς περιέχει το $\mathbb{Q}$.

Ορισμός Α΄.37. Έστω X ένα μη κενό σύνολο και $\sim$ μια σχέση ισοδυναμίας σ' αυτό. Αν $x \in \mathrm{X}$, τότε ορίζουμε την **κλάση ισοδυναμίας** $\mathrm{Cl}(x)$ του x ως το σύνολο των στοιχείων του X, τα οποία είναι ισοδύναμα με το x, δηλαδή $\mathrm{Cl}(x) = \{y \in \mathrm{X} \mid y \sim x\}$. Προφανώς $x \in \mathrm{Cl}(x)$, αφού $x \sim x$.

Πρόταση Α΄.38. Έστω X ένα μη κενό σύνολο και $\sim$ μια σχέση ισοδυναμίας σ' αυτό. Τα επόμενα είναι ισοδύναμα:
(i) $x \sim y$.
(ii) $y \in \mathrm{Cl}(x)$.
(iii) $\mathrm{Cl}(x) = \mathrm{Cl}(y)$.
(iv) $\mathrm{Cl}(x) \cap \mathrm{Cl}(y) \neq \varnothing$.
Απόδειξη: (i) $\Leftrightarrow$ **(ii)** Άμεση, από τον ορισμό της κλάσης ισοδυναμίας.
(i) $\Leftrightarrow$ **(iii)** Έστω $x \sim y$. Έστω $z \in \mathrm{Cl}(x) \Leftrightarrow z \sim x$. Επειδή $x \sim y$, λόγω της μεταβατικότητας της $\sim$,

$z \sim y \Leftrightarrow z \in \mathrm{Cl}(y)$. Άρα $\mathrm{Cl}(x) \subseteq \mathrm{Cl}(y)$. Αντιστρόφως, έστω $z \in \mathrm{Cl}(y) \Leftrightarrow z \sim y$. Επειδή $x \sim y \Leftrightarrow y \sim x$, λόγω της μεταβατικότητας της $\sim$, $z \sim x \Leftrightarrow z \in \mathrm{Cl}(x)$. Άρα $\mathrm{Cl}(y) \subseteq \mathrm{Cl}(x)$. Τελικώς $\mathrm{Cl}(y) = \mathrm{Cl}(x)$.
Αντιστρόφως, αν $\mathrm{Cl}(y) = \mathrm{Cl}(x)$, τότε $y \in \mathrm{Cl}(y) = \mathrm{Cl}(x)$ και άρα $y \sim x$.
(iii) $\Leftrightarrow$ **(iv)** Εφόσον το $\mathrm{Cl}(x) = \mathrm{Cl}(y)$ είναι μη κενό ($x \in \mathrm{Cl}(x)$), $\mathrm{Cl}(y) = \mathrm{Cl}(x) \cap \mathrm{Cl}(y) = \mathrm{Cl}(x) \neq \varnothing$. Αντιστρόφως, έστω $z \in \mathrm{Cl}(x) \cap \mathrm{Cl}(y)$. Τότε $z \in \mathrm{Cl}(x) \underset{\textbf{(ii)}\Leftrightarrow\textbf{(iii)}}{\Leftrightarrow} \mathrm{Cl}(z) = \mathrm{Cl}(x)$. Ομοίως, $z \in \mathrm{Cl}(y) \underset{\textbf{(ii)}\Leftrightarrow\textbf{(iii)}}{\Leftrightarrow} \mathrm{Cl}(z) = \mathrm{Cl}(y)$. Τελικώς $\mathrm{Cl}(x) = \mathrm{Cl}(y) = \mathrm{Cl}(z)$. ■

Από την προηγούμενη πρόταση προκύπτει ότι μια σχέση ισοδυναμίας σ᾽ ένα (μη κενό) σύνολο σύνολο X χωρίζει το σύνολο αυτό σε μη κενά και ξένα μεταξύ τους υποσύνολα, τις κλάσεις ισοδυναμίας. Κάθε $x \in \mathrm{X}$ ανήκει σε μια μοναδική κλάση ισοδυναμίας. Κάθε στοιχείο x μιας κλάσης ισοδυναμίας λέγεται **αντιπρόσωπος** της κλάσης αυτής. Ολόκληρη η κλάση αποτελείται ακριβώς από τα στοιχεία του X που είναι ισοδύναμα με το x. Λέμε ότι το σύνολο των κλάσεων ισοδυναμίας αποτελεί μια **διαμέριση του X**.

Ορισμός Α΄.39. Έστω $\mathrm{X} \neq \varnothing$ και $\varnothing \neq \mathcal{A} \subseteq \mathcal{P}(\mathrm{X})$. Λέμε ότι το $\mathcal{A}$ αποτελεί μια **διαμέριση του X**, αν και μόνον αν ισχύουν τα παρακάτω:
(i) $\varnothing \notin \mathcal{A}$.
(ii) Για κάθε A, A′ $\in \mathcal{A}$ με A $\neq$ A′, ισχύει $\mathrm{A} \cap \mathrm{A}' = \varnothing$.
(iii) $\bigcup_{\mathrm{A} \in \mathcal{A}} \mathrm{A} = \mathrm{X}$.

Πρόταση Α΄.40. Έστω $\mathcal{A}$ μια διαμέριση ενός συνόλου X. Τότε η $\mathcal{A}$ ορίζει μια **μοναδική** σχέση ισοδυναμίας $\sim$ στο X, ως εξής: $x \sim y \Leftrightarrow$ υπάρχει A $\in \mathcal{A}$ τέτοιο, ώστε $x, y \in$ A.
Απόδειξη: Η ανακλαστική και η συμμετρική ιδιότητα προκύπτουν άμεσα. Όσον αφορά στη μεταβατική, υποθέτουμε ότι $x \sim y$ και $y \sim z$. Τότε υπάρχουν A, A′ $\in \mathcal{A}$ τέτοια, ώστε $x, y \in$ A και $y, z \in$ A′. Εφόσον $y \in \mathrm{A} \cap \mathrm{A}'$, η τομή $\mathrm{A} \cap \mathrm{A}'$ είναι μη κενή. Από τον ορισμό της διαμέρισης προκύπτει ότι A = A′. Άρα $x, z \in$ A και συνεπώς $x \sim z$. ■

Από τα παραπάνω προκύπτει ότι σε ένα μη κενό σύνολο X, το πλήθος των σχέσεων ισοδυναμίας που μπορούμε να ορίσουμε σ᾽ αυτό συμπίπτει με το πλήθος των διαμερίσεων αυτού. Αν $|\mathrm{X}| = n > 0$, θετικός ακέραιος, το πλήθος αυτό ισούται με τον λεγόμενο **αριθμό Bell**, B_n. Μερικές τιμές για τους αριθμούς Bell: $\mathrm{B}_1 = 1, \mathrm{B}_2 = 2, \mathrm{B}_3 = 5, \mathrm{B}_4 = 15, \mathrm{B}_5 = 52, ...$

Παράρτημα Β΄

Περί αλγεβρικών δομών-σύντομη επισκόπηση

Ορισμός Β΄.1. Έστω Α, Β και Γ μη κενά σύνολα. Μια **πράξη με σύνολο τιμών στο Γ** είναι μια απεικόνιση της μορφής $\star : \mathrm{A} \times \mathrm{B} \to \Gamma$. Στις πράξεις δεν γράφουμε $\star(\alpha, \beta)$ ή πιο σωστά $\star((\alpha, \beta))$, αλλά $\alpha \star \beta$. Αν $\mathrm{A} = \mathrm{B} = \Gamma$, τότε η πράξη $\star : \mathrm{A} \times \mathrm{A} \to \mathrm{A}$ λέγεται **εσωτερική πράξη του Α**.

Πράξεις έχουμε συναντήσει αρκετές φορές στα μαθηματικά. Οι συνήθεις πράξεις στα διάφορα αριθμοσύνολα, τα οποία έχουμε διδαχθεί από το δημοτικό σχολείο ακόμα, αλλά και οι καινούργιες πράξεις, όπως πρόσθεση-αφαίρεση διανυσμάτων, εσωτερικό γινόμενο διανυσμάτων, πρόσθεση και πολλαπλασιασμός πινάκων, ενώσεις και τομές συνόλων, σύνθεση συναρτήσεων είναι ήδη γνωστές. Για τις πράξεις χρησιμοποιούμε διάφορα σύμβολα, με συνηθέστερα τα $+, \cdot, \star, \circ, \diamond, \triangle, \oplus, \odot$ κτλ. Πολλές φορές όμως **χρησιμοποιούμε καταχρηστικά και για λόγους οικονομίας το ίδιο σύμβολο αναφερόμενοι σε διαφορετικές πράξεις**. Για παράδειγμα, το σύμβολο $+$ χρησιμοποιείται και για την πρόσθεση αριθμών, αλλά και διανυσμάτων, πινάκων, συναρτήσεων κτλ. Επίσης, το ίδιο ισχύει και για το σύμβολο του πολλαπλασιασμού $\cdot$. Το τελευταίο χρησιμοποιείται και για το εσωτερικό γινόμενο διανυσμάτων. Το αποτέλεσμα της τελευταίας αυτής πράξης δεν είναι διάνυσμα αλλά πραγματικός αριθμός. Δεν είναι ασυνήθιστο σε μια σχέση να χρησιμοποιείται το ίδιο σύμβολο, με διαφορετική σημασία κάθε φορά. Ο προσεκτικός σπουδαστής των μαθηματικών πρέπει να αναγνωρίζει τη σημασία του κάθε συμβόλου σε μια σχέση και να αποδίδει σε αυτό την πραγματική του έννοια, ενίοτε διαφορετική σε πολλές περιπτώσεις, χωρίς να δημιουργείται σύγχυση. Αλλιώς, θα έπρεπε να επινοήσουμε σωρεία διαφορετικών συμβόλων και τότε το μπέρδεμα θα ήταν μεγαλύτερο. Αποφεύγουμε τον όρο «εξωτερική πράξη» στην περίπτωση μιας πράξης $\star : \mathrm{B} \times \mathrm{A} \to \mathrm{A}$ γιατί, όπως στην περίπτωση των διανυσματικών χώρων, ο βαθμωτός πολλαπλασιασμός μπορεί να είναι εσωτερική πράξη. Για παράδειγμα, κάθε σώμα είναι διανυσματικός χώρος επί του εαυτού του. Το σύμβολο $\cdot$ του πολλαπλασιασμού συνήθως παραλείπεται.

Ορισμός Β΄.2. Έστω Α μη κενό σύνολο και $\star : \mathrm{A} \times \mathrm{A} \to \mathrm{A}$ μια εσωτερική πράξη στο Α.
(i) Αν $\alpha \star (\beta \star \gamma) = (\alpha \star \beta) \star \gamma$, για κάθε $\alpha, \beta, \gamma \in \mathrm{A}$, τότε η πράξη $\star$ λέγεται **προσεταιριστική**.
(ii) Αν $\alpha \star \beta = \beta \star \alpha$, για κάθε $\alpha, \beta \in \mathrm{A}$, τότε η πράξη $\star$ λέγεται **αντιμεταθετική** ή απλούστερα **μεταθετική**.

Παραδείγματα: 1) Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού αριθμών (ακεραίων, ρητών, πραγματικών) είναι προσεταιριστικές και μεταθετικές.
2) Στο σύνολο $\mathbb{R}^{m \times n}$ των $m \times n$ πραγματικών πινάκων η πρόσθεση είναι προσεταιριστική και μεταθετική.
3) Στο σύνολο $\mathbb{R}^{n \times n}$ των $n \times n$ τετραγωνικών πραγματικών πινάκων ο πολλαπλασιασμός είναι προσεταιριστικός **αλλά όχι μεταθετικός**.
4) Αν $\mathrm{A} = \mathcal{P}(\mathrm{X})$ είναι το δυναμοσύνολο ενός συνόλου Χ, τότε σ' αυτό οι πράξεις της ένωσης και της τομής των στοιχείων του (υποσυνόλων του Χ) είναι και προσεταιριστικές και μεταθετικές.
5) Η πράξη $-$ της αφαίρεσης σε οποιοδήποτε σύνολο που έχουμε ήδη μάθει δεν είναι ούτε προσεταιριστική ούτε μεταθετική.
6) Στο $\mathbb{R}$ ορίζουμε μια πράξη $\circ$ ως εξής: $x \circ y = x + y - xy$, για κάθε $x, y \in \mathbb{R}$. Παρατηρούμε ότι αν $x, y, z \in \mathbb{R}$, τότε $x \circ (y \circ z) = x \circ (y + z - yz) = x + (y + z - yz) - x(y + z - yz) = x + y + z - (xy + yz + zx) + xyz$ και $(x \circ y) \circ z = (x + y - xy) \circ z = (x + y - xy) + z - (x + y - xy)z = x + y + z - (xy + yz + zx) + xyz$.

Άρα η πράξη $\circ$ είναι προσεταιριστική. Επίσης, αν $x, y \in \mathbb{R}$, τότε $x \circ y = x + y - xy = y + x - yx = y \circ x$ και άρα η $\circ$ είναι και μεταθετική.
7) Αν X είναι ένα μη κενό σύνολο και A είναι το σύνολο των συναρτήσεων της μορφής $f : X \to X$, τότε η συνήθης σύνθεση $\circ$ των συναρτήσεων στο A είναι προσεταιριστική πράξη αλλά όχι (εν γένει) μεταθετική.

Ορισμός Β΄.3. Ένα ζεύγος $(A, \star)$, όπου $\star$ εσωτερική πράξη του A, λέγεται **ημιομάδα** αν η $\star$ είναι προσεταιριστική.

Ορισμός Β΄.4. Έστω A μη κενό σύνολο εφοδιασμένο με μια εσωτερική πράξη $\star$. Ένα στοιχείο $e \in A$ λέγεται **ουδέτερο στοιχείο ως προς την πράξη $\star$** αν και μόνον αν $e \star x = x \star e = x$, για κάθε $x \in A$.

Πρόταση Β΄.5. Το ουδέτερο στοιχείο μιας εσωτερικής πράξης είναι μοναδικό.
Απόδειξη: Έστω e και e' δύο ουδέτερα στοιχεία μιας εσωτερικής πράξης $\star$ του A. Από τον ορισμό του e προκύπτει (για $x = e'$) ότι $e \star e' = e'$. Επίσης, από τον ορισμό του ουδέτερου στοιχείου e' προκύπτει (για $x = e$) ότι $e \star e' = e$. Επομένως $e = e' = e \star e'$. ■

Παραδείγματα: 1) Στο σύνολο $\mathbb{R}$ των πραγματικών και στα γνωστά υποσύνολά του $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ το μηδέν (0) είναι το μοναδικό ουδέτερο στοιχείο της πρόσθεσης και το ένα (1) το μοναδικό ουδέτερο στοιχείο του πολλαπλασιασμού.
2) Στο σύνολο $\mathbb{R}^{m\times n}$ των $m \times n$ πινάκων ο μηδενικός πίνακας $\mathbf{O}_{m\times n}$ είναι το μοναδικό ουδέτερο στοιχείο της πρόσθεσης και στο σύνολο $\mathbb{R}^{n\times n}$ των $n \times n$ τετραγωνικών πινάκων ο μοναδιαίος πίνακας $\mathbf{I}_n$ είναι το μοναδικό ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό.
3) Στο δυναμοσύνολο $\mathcal{P}(\Omega)$ ενός βασικού συνόλου Ω, το $\varnothing$ είναι το μοναδικό ουδέτερο στοιχείο της ένωσης και το Ω το μοναδικό ουδέτερο στοιχείο της τομής.
4) Στο σύνολο A όλων των συναρτήσεων της μορφής $f : X \to X$, όπου $X \neq \varnothing$, η ταυτοτική συνάρτηση $1_X : X \to X$ είναι το μοναδικό ουδέτερο στοιχείο ως προς την πράξη της σύνθεσης συναρτήσεων.

Ορισμός Β΄.6. Έστω A μη κενό σύνολο εφοδιασμένο με μια εσωτερική πράξη $\star$. Υποθέτουμε επίσης ότι υπάρχει ουδέτερο στοιχείο $e \in A$ ως προς την $\star$. Αν για κάποιο $x \in A$ υπάρχει στοιχείο $\hat{x} \in A$ τέτοιο, ώστε $x \star \hat{x} = \hat{x} \star x = e$, τότε το $\hat{x}$ λέγεται **συμμετρικό του x** ως προς την πράξη $\star$.

Πρόταση Β΄.7. Σε μια ημιομάδα $(A, \star)$ με ουδέτερο στοιχείο e, το συμμετρικό ενός στοιχείου είναι μοναδικό.
Απόδειξη: Έστω $x \in A$ και $\hat{x}, \bar{x} \in A$ τέτοια, ώστε $x \star \hat{x} = \hat{x} \star x = e$ και $x \star \bar{x} = \bar{x} \star x = e$. Παρατηρούμε ότι: $\hat{x} = \hat{x} \star e = \hat{x} \star (x \star \bar{x}) = (\hat{x} \star x) \star \bar{x} = e \star \bar{x} = \bar{x}$. ■

Ορισμός Β΄.8. Έστω G ένα μη κενό σύνολο εφοδιασμένο με μια εσωτερική πράξη $\star$. Το ζεύγος $(G, \star)$ λέγεται **ομάδα** αν και μόνον αν ισχύουν τα ακόλουθα:
(i) Το ζεύγος $(G, \star)$ είναι ημιομάδα, δηλαδή για κάθε $x, y, z \in G$ ισχύει η σχέση: $x \star (y \star z) = (x \star y) \star z$.
(ii) Υπάρχει ουδέτερο στοιχείο e ως προς την πράξη $\star$, δηλαδή $e \star x = x \star e = x$, για κάθε $x \in G$.
(iii) Για κάθε $x \in G$ υπάρχει συμμετρικό $\hat{x}$, δηλαδή $x \star \hat{x} = \hat{x} \star x = e$.

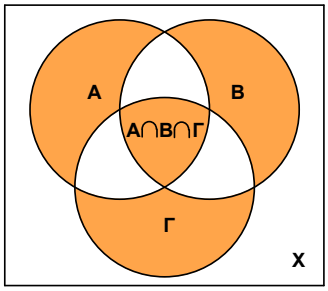
Ορισμός Β΄.9. Μια ομάδα $(G, \star)$ λέγεται **αντιμεταθετική** ή **αβελιανή**[1] αν η πράξη $\star$ είναι μεταθετική.

Στα επόμενα, όταν είναι σαφής η εσωτερική πράξη, θα λέμε απλώς η ομάδα G αντί η ομάδα $(G, \star)$.
Παραδείγματα: 1) Τα σύνολα των ακεραίων, των ρητών και των πραγματικών είναι αβελιανές ομάδες ως προς την πρόσθεση. Το συμμετρικό ενός στοιχείου x είναι το αντίθετό του $-x$. Το σύνολο των φυσικών δεν είναι ομάδα ως προς την πρόσθεση, γιατί ο αντίθετος ενός φυσικού, πχ. του 1, δεν είναι πάντα φυσικός.
2) Τα σύνολα $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ και $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ είναι αβελιανές ομάδες. Το συμμετρικό ενός στοιχείου τους είναι το αντίστροφό του. Το $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ δεν είναι ομάδα ως προς τον πολλαπλασιασμό, γιατί ο αντίστροφος ενός ακεραίου, διαφορετικού του ± 1 δεν είναι ακέραιος.
3) Έστω X ένα μη κενό σύνολο. Το σύνολο όλων των **1-1 και επί** απεικονίσεων της μορφής $f : X \to X$

[1] Προς τιμή του μεγάλου Νορβηγού μαθηματικού Niels Henrik Abel (1802-1829)!

είναι ομάδα με πράξη τη σύνθεση $\circ$ απεικονίσεων. Αυτές οι απεικονίσεις λέγονται **μεταθέσεις του Χ**. Το συμμετρικό μιας απεικόνισης $f : X \to X$ είναι η αντίστροφη αυτής $f^{-1} : X \to X$. Η ομάδα των μεταθέσεων του Χ λέγεται **η συμμετρική ομάδα του Χ** και συμβολίζεται με Sym(Χ) ή S_X. Αν το Χ περιέχει ακριβώς $n \geq 1$ στοιχεία, για παράδειγμα όταν Χ$= \{1, 2, 3, \ldots, n\}$, η S_X συμβολίζεται με S_n. Η S_n αποτελείται από $n!$ μεταθέσεις. Για $n \geq 3$ η S_n **δεν είναι αβελιανή**.

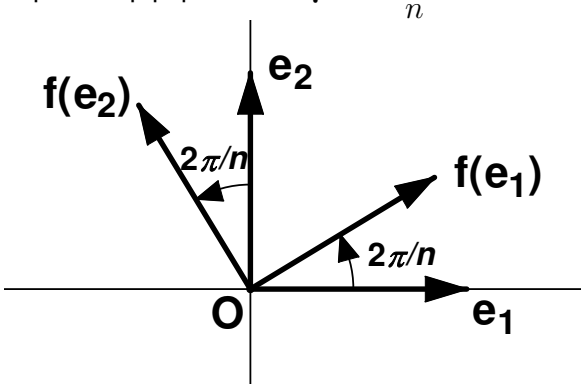
4) Έστω $\mathcal{P}(X)$ το δυναμοσύνολο ενός συνόλου Χ. Ορίζουμε στο $\mathcal{P}(X)$ την πράξη $\triangle$ της συμμετρικής διαφοράς, ως εξής: $A\triangle B = (A\setminus B)\cup(B\setminus A) = (A\cup B)\setminus(A\cap B) = (A\cup B)\cap(A\cap B)^c$. Τότε το ζεύγος $(\mathcal{P}(X), \triangle)$ είναι αβελιανή ομάδα. Προφανώς η πράξη $\triangle$ είναι μεταθετική. Θα αποδείξουμε ότι είναι και προσεταιριστική. Γι' αυτό θα χρησιμοποιήσουμε τα αποτελέσματα της πρότασης Α΄.16. Πράγματι, έστω $A, B, \Gamma \subseteq X$.
Τότε $A\triangle(B\triangle\Gamma) = (A \setminus (B\triangle\Gamma)) \cup ((B\triangle\Gamma) \setminus A)$. Τώρα, $A \setminus (B\triangle\Gamma) = A \setminus ((B \setminus \Gamma) \cup (\Gamma \setminus B)) = (A \setminus (B \setminus \Gamma))\cap$ $\cap(A\setminus(\Gamma\setminus B)) = [(A\setminus B)\cup(A\cap\Gamma)]\cap[(A\setminus\Gamma)\cup(A\cap B)] = [(A\setminus B)\cap(A\setminus\Gamma)]\cup[(A\setminus B)\cap(A\cap B)]\cup[(A\cap\Gamma)\cap(A\setminus\Gamma)]\cup$ $\cup[(A\cap\Gamma)\cap(A\cap B)] = (A \setminus (B\cup\Gamma))\cup\varnothing\cup\varnothing\cup(A\cap B\cap\Gamma) = (A \setminus (B\cup\Gamma))\cup(A\cap B\cap\Gamma)$.
Επίσης, $(B\triangle\Gamma) \setminus A = [(B \setminus \Gamma) \cup (\Gamma \setminus B)] \setminus A = [(B \setminus \Gamma) \setminus A] \cup [(\Gamma \setminus B) \setminus A] = (B \setminus (A\cup\Gamma)) \cup (\Gamma \setminus (A\cup B))$.
Επομένως $A\triangle(B\triangle\Gamma) = (A \setminus (B\triangle\Gamma))\cup((B\triangle\Gamma) \setminus A) = (A \setminus (B\cup\Gamma))\cup(B \setminus (\Gamma\cup A))\cup(\Gamma \setminus (A\cup B))\cup(A\cap B\cap\Gamma)$.
Παρατηρούμε ότι η τελευταία παράσταση είναι συμμετρική ως προς Α, Β και Γ. Άρα και το αποτέλεσμα $\Gamma\triangle(A\triangle B)$ θα είναι το ίδιο, δηλαδή $A\triangle(B\triangle\Gamma) = \Gamma\triangle(A\triangle B)$ και λόγω της αντιμεταθετικότητας, το τελευταίο ισούται με $(A\triangle B)\triangle\Gamma$.



Σχήμα 6

Το ουδέτερο στοιχείο είναι το $\varnothing$ αφού, για κάθε $A \in \mathcal{P}(X)$ έχουμε: $A\triangle\varnothing = \varnothing\triangle A = (A \setminus \varnothing) \cup (\varnothing \setminus A) =$ $= A \cup \varnothing = A$.
Το συμμετρικό κάθε $A \in \mathcal{P}(X)$ είναι ο εαυτός του. Πράγματι, $A\triangle A = (A \setminus A) \cup (A \setminus A) = \varnothing \cup \varnothing = \varnothing$.

5) Θεωρούμε τον πίνακα $A = \begin{pmatrix} \text{συν}\frac{2\pi}{n} & -\text{ημ}\frac{2\pi}{n} \\ \text{ημ}\frac{2\pi}{n} & \text{συν}\frac{2\pi}{n} \end{pmatrix}$, όπου $n \geq 2$. Ο πίνακας αυτός παριστάνει στο επίπεδο $\mathbb{R}^2$ μια στροφή f, κατά τη θετική φορά, κατά γωνία $\frac{2\pi}{n}$.



Σχήμα 7

Μπορούμε να αποδείξουμε (με επαγωγή-βλέπε επόμενο παράρτημα) ότι $\mathrm{A}^k = \begin{pmatrix} \text{συν}\frac{2k\pi}{n} & -\text{ημ}\frac{2k\pi}{n} \\ \text{ημ}\frac{2k\pi}{n} & \text{συν}\frac{2k\pi}{n} \end{pmatrix}$, για κάθε $k = 1, 2, \ldots, n$. Επίσης $\mathrm{A}^n = \mathrm{I}_n$, ο ταυτοτικός πίνακας. Το σύνολο $\mathrm{G} = \{\mathrm{A}^k \mid k = 0, 1, 2, \ldots, n-1\}$ αποτελεί ομάδα με πράξη τον πολλαπλασιασμό πινάκων. Το πλήθος των στοιχείων της, το οποίο ονομάζεται **τάξη της ομάδας** είναι n. Η ομάδα αυτή παράγεται από τον πίνακα Α, υπό την έννοια ότι αποτελείται από δυνάμεις του Α. Μια τέτοια ομάδα λέγεται **κυκλική τάξης n**. Το ουδέτερο στοιχείο είναι ο ταυτοτικός πίνακας I_n και ο αντίστροφος του A^k είναι ο A^{n-k}.

Πρόταση Β΄.10. Έστω $(\mathrm{G}, \star)$ μια ομάδα. Τότε ισχύουν τα εξής:
(i) (Νόμοι της διαγραφής) Για κάθε $\alpha, \beta, \gamma \in \mathrm{G}$ ισχύουν οι ακόλουθες ισοδυναμίες:
α) $\alpha \star \beta = \alpha \star \gamma \Leftrightarrow \beta = \gamma$ και **β)** $\beta \star \alpha = \gamma \star \alpha \Leftrightarrow \beta = \gamma$.
(ii) Για κάθε $\alpha, \beta \in \mathrm{G}$ οι εξισώσεις $\alpha \star x = \beta$ και $y \star \alpha = \beta$ έχουν μοναδική λύση.
Απόδειξη: Έστω e το ουδέτερο στοιχείο της G και $\hat{\alpha}$ το συμμετρικό του α ως προς την πράξη $\star$.
(i) Οι συνεπαγωγές $\beta = \gamma \Rightarrow \alpha \star \beta = \alpha \star \gamma$ και $\beta = \gamma \Rightarrow \beta \star \alpha = \gamma \star \alpha$ είναι προφανείς. Θα αποδείξουμε τις αντίστροφες συνεπαγωγές. Έστω $\alpha \star \beta = \alpha \star \gamma$. Τότε $\hat{\alpha} \star (\alpha \star \beta) = \hat{\alpha} \star (\alpha \star \gamma) \underset{\star \text{ προσεταιριστική}}{\Leftrightarrow} (\hat{\alpha} \star \alpha) \star \beta = (\hat{\alpha} \star \alpha) \star \gamma \Leftrightarrow e \star \beta = e \star \gamma \Leftrightarrow \beta = \gamma$. Ομοίως, $\beta \star \alpha = \gamma \star \alpha \Rightarrow (\beta \star \alpha) \star \hat{\alpha} = (\gamma \star \alpha) \star \hat{\alpha} \Leftrightarrow \beta \star (\alpha \star \hat{\alpha}) = \gamma \star (\alpha \star \hat{\alpha}) \Leftrightarrow \beta \star e = \gamma \star e \Leftrightarrow \beta = \gamma$.
(ii) Από τους νόμους της διαγραφής έχουμε: $\alpha \star x = \beta \Leftrightarrow \hat{\alpha} \star (\alpha \star x) = \hat{\alpha} \star \beta \Leftrightarrow (\hat{\alpha} \star \alpha) \star x = \hat{\alpha} \star \beta \Leftrightarrow e \star x = \hat{\alpha} \star \beta \Leftrightarrow x = \hat{\alpha} \star \beta$. Ομοίως, $y \star \alpha = \beta \Leftrightarrow (y \star \alpha) \star \hat{\alpha} = \beta \star \hat{\alpha} \Leftrightarrow y \star (\alpha \star \hat{\alpha}) = \beta \star \hat{\alpha} \Leftrightarrow y \star e = \beta \star \hat{\alpha} \Leftrightarrow y = \beta \star \hat{\alpha}$. ■

Αν η ομάδα G είναι αβελιανή, τότε: **1)** Αν η πράξη συμβολίζεται με $+$ και φυσικά θα λέγεται πρόσθεση, τότε ορίζεται μια νέα πράξη, η οποία λέγεται **αφαίρεση**, ως εξής: $x - y = x + (-y)$. **2)** Αν η πράξη συμβολίζεται με $\cdot$ και φυσικά θα λέγεται πολλαπλασιασμός, τότε ορίζεται μια νέα πράξη, η οποία λέγεται **διαίρεση**, ως εξής: $x : y = \frac{x}{y} = xy^{-1}$. Η αφαίρεση και η διαίρεση είναι λοιπόν **παράγωγες** πράξεις, οι οποίες ορίζονται σε μια αβελιανή ομάδα μέσω της πρόσθεσης και του πολλαπλασιασμού αντίστοιχα.

Ορισμός Β΄.11. Έστω Α ένα μη κενό σύνολο εφοδιασμένο με δύο πράξεις $\star$ και $\circ$. Η πράξη $\circ$ λέγεται **αριστερά επιμεριστική** ως προς την πράξη $\star$ αν, για κάθε $x, y, z \in \mathrm{A}$ ισχύει η σχέση: $x \circ (y \star z) = (x \circ y) \star (x \circ z)$. Ανάλογα, η πράξη $\circ$ λέγεται **δεξιά επιμεριστική** ως προς την πράξη $\star$ αν, για κάθε $x, y, z \in \mathrm{A}$ ισχύει η σχέση: $(y \star z) \circ x = (y \circ x) \star (z \circ x)$. Αν η $\circ$ είναι και δεξιά και αριστερά επιμεριστική ως προς την $\star$, τότε η $\circ$ λέγεται απλώς **επιμεριστική** ως προς την $\star$.

Παραδείγματα: 1) Ο συνήθης πολλαπλασιασμός αριθμών (φυσικών, ακεραίων, ρητών, πραγματικών) είναι επιμεριστικός ως προς την αντίστοιχη πρόσθεση.
2) Στο δυναμοσύνολο $\mathcal{P}(\mathrm{X})$ ενός συνόλου X η ένωση είναι επιμεριστική ως προς την τομή, αλλά και η τομή είναι επιμεριστική ως προς την ένωση.
3) Στο σύνολο $\mathbb{F}$ των τετραγωνικών $n \times n$ πινάκων, όπου $\mathbb{F}$ μπορεί να είναι κάποιο από τα γνωστά αριθμοσύνολα $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση.

Ορισμός Β΄.12. Θεωρούμε ένα (μη κενό) σύνολο R εφοδιασμένο με δύο πράξεις $+$ και $\cdot$. Την πράξη $+$ θα τη λέμε ως συνήθως **πρόσθεση** και την πράξη $\cdot$ **πολλαπλασιασμό**. Υποθέτουμε τα εξής:
α) Το ζεύγος $(\mathrm{R}, +)$ είναι αβελιανή ομάδα. Δηλαδή:
(i) $x + y = y + x$, για κάθε $x, y \in \mathrm{R}$.
(ii) $x + (y + z) = (x + y) + z$, για κάθε $x, y, z \in \mathrm{R}$.
(iii) Υπάρχει ουδέτερο στοιχείο, το οποίο ως συνήθως συμβολίζεται με 0, τέτοιο ώστε $x + 0 = x$, για κάθε $x \in \mathrm{R}$. (Η σχέση $0 + x = x$ είναι περιττή, αφού η ομάδα $(\mathrm{R}, +)$ είναι αβελιανή).
(iv) Για κάθε $x \in \mathrm{R}$ υπάρχει (μοναδικό) στοιχείο $-x$ τέτοιο, ώστε $x + (-x) = 0$. (Και εδώ, για τον ίδιο λόγο, η σχέση $(-x) + x = 0$ είναι περιττή).

β) Το ζεύγος $(\mathrm{R},\cdot)$ είναι ημιομάδα, δηλαδή ο πολλαπλασιασμός είναι προσεταιριστικός, δηλαδή
(v) $x(yz)=(xy)z$, για κάθε $x,y,z\in\mathrm{R}$.
γ) Ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση, δηλαδή
(vi) $x(y+z)=xy+xz$ και $(x+y)z=xz+yz$, για κάθε $x,y,z\in\mathrm{R}$.
Τότε το σύνολο R ή ακριβέστερα η τριάδα $(\mathrm{R},+,\cdot)$ λέγεται **δακτύλιος**.
Αν ο πολλαπλασιασμός είναι μεταθετικός, ήτοι $xy=yx$, για κάθε $x,y\in\mathrm{R}$, τότε ο δακτύλιος R λέγεται **μεταθετικός δακτύλιος**.
Αν ο πολλαπλασιασμός έχει ουδέτερο στοιχείο, το οποίο συμβολίζεται ως συνήθως με 1, τότε ο δακτύλιος λέγεται **μοναδιαίος** ή **δακτύλιος με μονάδα**.
Τέλος, αν ο δακτύλιος είναι και μεταθετικός, αλλά και μοναδιαίος, τότε λέγεται **μοναδιαίος μεταθετικός δακτύλιος** ή **μεταθετικός δακτύλιος με μονάδα**.

Παρατηρούμε ότι το μονοσύνολο $\{0\}$ πληροί τα αξιώματα ενός μεταθετικού δακτυλίου με μονάδα. Εδώ το 0 και το 1 ταυτίζονται! Ο δακτύλιος αυτός λέγεται **τετριμμένος δακτύλιος**. Στα επόμενα, με τον όρο δακτύλιο θα εννοούμε έναν μη τετριμμένο δακτύλιο, δηλαδή να περιέχει δύο τουλάχιστον στοιχεία.
Παραδείγματα: 1) Οι ακέραιοι, οι ρητοί και οι πραγματικοί αποτελούν (με τις προφανείς πράξεις) μοναδιαίους μεταθετικούς δακτυλίους.
2) Το σύνολο $\mathbb{F}$ των τετραγωνικών $n\times n$ πινάκων, όπου $\mathbb{F}$ μπορεί να είναι κάποιο από τα γνωστά αριθμοσύνολα $\mathbb{Z},\mathbb{Q},\mathbb{R}$ με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού πινάκων είναι μοναδιαίος δακτύλιος. **Δεν είναι όμως μεταθετικός**. Για παράδειγμα, στο $\mathbb{Z}^{2\times2}$ έχουμε

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}=\begin{pmatrix}2&1\\1&1\end{pmatrix},\ \text{αλλά}\ \begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&1\\1&2\end{pmatrix}.$$

3) Αν A είναι ένα μη κενό σύνολο και $\mathbb{R}^{\mathrm{A}}$ είναι το σύνολο των συναρτήσεων $f:\mathrm{A}\to\mathbb{R}$, τότε το $\mathbb{R}^{\mathrm{A}}$ με πράξεις τις πράξεις $+$ και $\cdot$, όπου $(f+g)(x)=f(x)+g(x)$ και $(fg)(x)=f(x)g(x)$, για κάθε $x\in\mathrm{A}$ είναι μοναδιαίος μεταθετικός δακτύλιος. Το μηδενικό στοιχείο είναι η συνάρτηση $\mathbf{0}:\mathrm{A}\to\mathbb{R}$ με $\mathbf{0}(x)=0$, για κάθε $x\in\mathrm{A}$ και μονάδα η συνάρτηση $\mathbf{1}:\mathrm{A}\to\mathbb{R}$ με $\mathbf{1}(x)=1$, για κάθε $x\in\mathrm{A}$. Χρησιμοποιήσαμε **bold** στοιχεία προς αποφυγήν συγχύσεως. Μάλλον δεν ήταν αναγκαίο.
4) Οι δακτύλιοι δεν είναι κατ' ανάγκην άπειρα σύνολα. Για παράδειγμα στο σύνολο $\{0,1\}$ ορίζουμε τις πράξεις $\oplus$ (πρόσθεση) και $\cdot$ (πολλαπλασιασμός), όπως φαίνεται στους παρακάτω πίνακες:

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Το σύνολο $\{0,1\}$, το οποίο ας συμβολίσουμε με $\mathbb{Z}_2$, αποτελεί ως προς τις παραπάνω πράξεις έναν μεταθετικό δακτύλιο με μονάδα. Βλέπετε, αποφύγαμε τη χρήση του συμβόλου $+$ για την πρόσθεση, επειδή κάποιος μπορεί να μπερδευτεί και να θεωρήσει ότι η σχέση $1+1=0$ ισχύει στους ακεραίους αριθμούς! Θα μπορούσαμε να κρατήσουμε για την πρόσθεση το σύμβολο $+$ και να γράφαμε $\{\langle0\rangle,\langle1\rangle\}$ αντί $\{0,1\}$. Τα σύμβολα $\langle0\rangle$ και $\langle1\rangle$ εκφράζουν συγκεκριμένες έννοιες: Το $\langle0\rangle$ εκφράζει την κλάση των **αρτίων ακεραίων** και το $\langle1\rangle$ την κλάση των **περιττών**. Έτσι, οι πίνακες

$+$	$\langle0\rangle$	$\langle1\rangle$
$\langle0\rangle$	$\langle0\rangle$	$\langle1\rangle$
$\langle1\rangle$	$\langle1\rangle$	$\langle0\rangle$

$\cdot$	$\langle0\rangle$	$\langle1\rangle$
$\langle0\rangle$	$\langle0\rangle$	$\langle0\rangle$
$\langle1\rangle$	$\langle0\rangle$	$\langle1\rangle$

εκφράζουν τους κανόνες: «άρτιος + άρτιος = άρτιος», «άρτιος + περιττός = περιττός», «περιττός + περιττός = άρτιος» (1+1=0), «άρτιος · άρτιος = άρτιος», «άρτιος · περιττός = άρτιος» και «περιττός · περιττός = περιττός».
5) Έστω X ένα μη κενό σύνολο. Τότε το $\mathcal{P}(\mathrm{X})$ περιέχει προφανώς δύο τουλάχιστον στοιχεία: το X και το $\varnothing$. Γνωρίζουμε ότι η $(\mathcal{P}(\mathrm{X}),\triangle)$ είναι αβελιανή ομάδα. (βλέπε παράδειγμα 4 μετά τον ορισμό της ομάδας). Η $\triangle$ θα είναι η «πρόσθεσή» μας στο $\mathcal{P}(\mathrm{X})$. Το μηδενικό στοιχείο στο $(\mathcal{P}(\mathrm{X}),\triangle)$ είναι το $\varnothing$ και το αντίθετο

ενός $A \in \mathcal{P}(X)$ είναι το ίδιο το A. Η τομή $\cap$ θα είναι ο «πολλαπλασιασμός» μας. Γνωρίζουμε ότι η τομή είναι αντιμεταθετική και προσεταιριστική πράξη στο $\mathcal{P}(X)$. Θα αποδείξουμε ότι η τομή είναι επιμεριστική ως προς τη συμμετρική διαφορά $\triangle$. Παρατηρούμε ότι: $(A\cap B)\setminus(A\cap\Gamma) = (A\cap B)\cap(A\cap\Gamma)^c = (A\cap B)\cap$ $\cap(A^c\cup\Gamma^c) = (A\cap B\cap A^c)\cup(A\cap B\cap\Gamma^c) = (B\cap\varnothing)\cup(A\cap B\cap\Gamma^c) = \varnothing\cup(A\cap B\cap\Gamma^c) = A\cap B\cap\Gamma^c$. Παρόμοια παίρνουμε: $(A\cap\Gamma)\setminus(A\cap B) = A\cap\Gamma\cap B^c$. Επομένως $A\cap(B\triangle\Gamma) = A\cap[(B\setminus\Gamma)\cup(\Gamma\setminus B)] = A\cap[(B\cap\Gamma^c)\cup$ $\cup(\Gamma\cap B^c)] = (A\cap B\cap\Gamma^c)\cup(A\cap\Gamma\cap B^c) = [(A\cap B)\setminus(A\cap\Gamma)]\cup[(A\cap\Gamma)\setminus(A\cap B)] = (A\cap B)\triangle(A\cap\Gamma)$. Επειδή η τομή είναι μεταθετική πράξη στο $\mathcal{P}(X)$, θα έχουμε: $(A\triangle B)\cap\Gamma = \Gamma\cap(A\triangle B) = (\Gamma\cap A)\triangle(\Gamma\cap B) = (A\cap\Gamma)\triangle(B\cap\Gamma)$. Άρα η τομή είναι επιμεριστική ως προς τη συμμετρική διαφορά. Η τριάδα λοιπόν $(\mathcal{P}(X),\triangle,\cap)$ είναι μεταθετικός δακτύλιος. Επιπλέον είναι μοναδιαίος με μονάδα το X, αφού $A\cap X = A$, για κάθε $A\in\mathcal{P}(X)$.

Αν υποθέσουμε ότι το X είναι μονοσύνολο, ήτοι $X=\{x\}$, τότε $\mathcal{P}(X)=\{\varnothing, X\}$. Οι πίνακες της συμμετρικής διαφοράς $\triangle$ και της τομής $\cap$ είναι οι ακόλουθοι:

$\triangle$	$\varnothing$	X
$\varnothing$	$\varnothing$	X
X	X	$\varnothing$

$\cap$	$\varnothing$	X
$\varnothing$	$\varnothing$	$\varnothing$
X	$\varnothing$	X

Προσέξτε την ομοιότητα με τους πίνακες των πράξεων του προηγούμενου παραδείγματος! Σ' αυτή την περίπτωση λέμε ότι οι δακτύλιοι $(\mathbb{Z}_2,+,\cdot)$ και $(\mathcal{P}(X),\triangle,\cap)$ είναι **ισόμορφοι**.

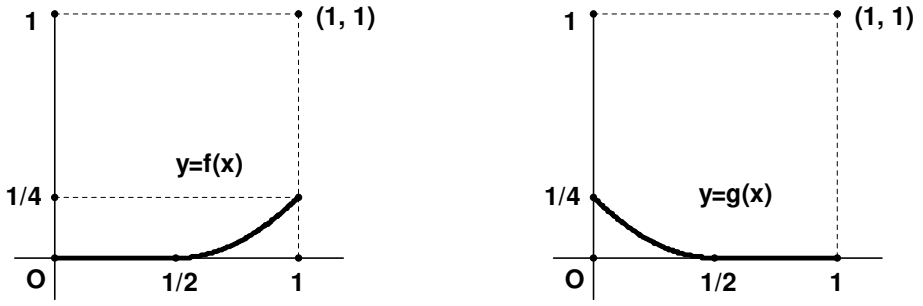
Πρόταση Β΄.13. Σε κάθε δακτύλιο $(R,+,\cdot)$ (μεταθετικό ή μη) ισχύουν τα ακόλουθα:
(i) $\alpha\cdot 0 = 0\cdot\alpha = 0$, για κάθε $\alpha\in R$.
(ii) $(-\alpha)\beta = \alpha(-\beta) = -\alpha\beta$, για κάθε $\alpha,\beta\in R$.
Απόδειξη: (i) $\alpha\cdot 0 = \alpha\cdot(0+0) = \alpha\cdot 0+\alpha\cdot 0$, δηλαδή $\alpha\cdot 0 = \alpha\cdot 0+\alpha\cdot 0 \Rightarrow \alpha\cdot 0+(-(\alpha\cdot 0)) =$ $= (\alpha\cdot 0+\alpha\cdot 0)+(-(\alpha\cdot 0)) \Leftrightarrow 0 = \alpha\cdot 0+(\alpha\cdot 0+(-(\alpha\cdot 0))) \Leftrightarrow 0 = \alpha\cdot 0+0 = \alpha\cdot 0$.
Ανάλογα έχουμε: $0\cdot a = (0+0)\cdot a = 0\cdot a+0\cdot a \Rightarrow 0\cdot a-0\cdot a = (0\cdot a+0\cdot a)-0\cdot a \Leftrightarrow 0 = 0\cdot a+(0\cdot a-0\cdot a) \Leftrightarrow$ $\Leftrightarrow 0 = 0\cdot a+0 = 0\cdot a$.
(ii) $(-\alpha)\beta+\alpha\beta = (-\alpha+\alpha)\beta = 0\cdot\beta = 0$. Επομένως $(-\alpha)\beta = -\alpha\beta$. Ανάλογα, $\alpha(-\beta)+\alpha\beta = \alpha(-\beta+\beta) =$ $= \alpha\cdot 0 = 0$. Άρα $\alpha(-\beta) = -\alpha\beta$. ■

Ορισμός Β΄.14. Έστω $(R,+,\cdot)$ ένας μοναδιαίος μεταθετικός δακτύλιος. Ο R λέγεται **ακέραια περιοχή** αν από κάθε σχέση της μορφής $\alpha\beta = 0$, όπου $\alpha,\beta\in R$, προκύπτει ότι $\alpha = 0$ ή $\beta = 0$.

Παραδείγματα: 1) Οι δακτύλιοι των ακεραίων, ρητών, πραγματικών είναι προφανώς ακέραιες περιοχές.
2) Ο δακτύλιος $(\mathbb{Z}_2,+,\cdot)$ που ορίστηκε παραπάνω είναι ακέραια περιοχή, όπως μπορεί κανείς να διαπιστώσει με ευκολία, ελέγχοντας τον πίνακα του πολλαπλασιασμού. Το ίδιο προφανώς ισχύει και για τον δακτύλιο $(\mathcal{P}(X),\triangle,\cap)$, όταν το X είναι μονοσύνολο. Αν όμως το X περιέχει δύο τουλάχιστον στοιχεία, τότε ο $(\mathcal{P}(X),\triangle,\cap)$ **δεν είναι ακέραια περιοχή**. Πράγματι, αν $\alpha,\beta\in X$ με $\alpha\neq\beta$, τότε $\{\alpha\}\cap\{\beta\} = \varnothing$, ενώ $\{\alpha\}\neq\varnothing$ και $\{\beta\}\neq\varnothing$.
3) Έστω $C([0,1])$ το σύνολο των συνεχών συναρτήσεων $f:[0,1]\to\mathbb{R}$. Το $C([0,1])$ είναι ένας μεταθετικός δακτύλιος με τις προφανείς πράξεις: $f+g:[0,1]\to\mathbb{R}$ και $fg:[0,1]\to\mathbb{R}$, όπου $(f+g)(x) = f(x)+g(x)$ και $(fg)(x) = f(x)g(x)$, για κάθε $x\in[0,1]$. Μηδενικό στοιχείο είναι η συνάρτηση $\mathbf{0}:[0,1]\to\mathbb{R}$ με $\mathbf{0}(x) = 0$, για κάθε $x\in[0,1]$ και μοναδιαίο στοιχείο η συνάρτηση $\mathbf{1}:[0,1]\to\mathbb{R}$ με $\mathbf{1}(x) = 1$, για κάθε $x\in[0,1]$. Θεωρούμε τις συνεχείς συναρτήσεις $f,g\in C([0,1])$ με

$$f(x) = \begin{cases} 0, & \text{αν } 0\le x<\dfrac{1}{2} \\ \left(x-\dfrac{1}{2}\right)^2, & \text{αν } \dfrac{1}{2}\le x\le 1 \end{cases} \qquad \text{και} \qquad g(x) = \begin{cases} \left(x-\dfrac{1}{2}\right)^2, & \text{αν } 0\le x<\dfrac{1}{2} \\ 0, & \text{αν } \dfrac{1}{2}\le x\le 1 \end{cases}$$

Μάλιστα, οι συναρτήσεις αυτές είναι παραγωγίσιμες. Προφανώς $f,g\neq\mathbf{0}$, αλλά $fg = \mathbf{0}$. Επομένως το $C([0,1])$ δεν είναι ακέραια περιοχή. Οι γραφικές παραστάσεις των f και g είναι οι ακόλουθες:



Σχήμα 8

Ορισμός Β΄.15. Έστω $(\mathrm{R}, +, \cdot)$ ένας μοναδιαίος μεταθετικός δακτύλιος. Έστω $\mathrm{R}^* = \mathrm{R} \setminus \{0\}$ το σύνολο των μη μηδενικών στοιχείων του. Προφανώς $1 \in \mathrm{R}^*$. Αν το R^* εφοδιασμένο με την πράξη $\cdot$ του πολλαπλασιασμού είναι (αβελιανή) ομάδα, τότε ο δακτύλιος $(\mathrm{R}, +, \cdot)$ λέγεται **σώμα**.

Με άλλα λόγια, ένας μοναδιαίος μεταθετικός δακτύλιος είναι σώμα αν και μόνον αν κάθε μη μηδενικό στοιχείο του έχει αντίστροφο. Το αντίστροφο ενός $\alpha \in \mathrm{R}^*$ συμβολίζεται ως συνήθως με α^{-1}. Αναφέρουμε αναλυτικά τις ιδιότητες του σώματος:

(i) $x + y = y + x$, για κάθε $x, y \in \mathrm{R}$.
(ii) $x + (y + z) = (x + y) + z$, για κάθε $x, y, z \in \mathrm{R}$.
(iii) Υπάρχει προσθετικό ουδέτερο στοιχείο, το οποίο ως συνήθως συμβολίζεται με 0, τέτοιο ώστε $x+0 = x$, για κάθε $x \in \mathrm{R}$.
(iv) Για κάθε $x \in \mathrm{R}$ υπάρχει (μοναδικό) στοιχείο $-x$ τέτοιο, ώστε $x + (-x) = 0$.
(v) $x(yz) = (xy)z$, για κάθε $x, y, z \in \mathrm{R}$.
(vi) $xy = yx$, για κάθε $x, y \in \mathrm{R}$.
(vii) $x(y + z) = xy + xz$, για κάθε $x, y, z \in \mathrm{R}$.
(viii) Υπάρχει πολλαπλασιαστικό ουδέτερο στοιχείο, το οποίο ως συνήθως συμβολίζεται με 1, τέτοιο ώστε $x \cdot 1 = x$, για κάθε $x \in \mathrm{R}$.
(ix) Για κάθε $x \in \mathrm{R}^* = \mathrm{R} \setminus \{0\}$ υπάρχει (μοναδικό) στοιχείο x^{-1} τέτοιο, ώστε $x \cdot x^{-1} = 1$.

Πρόταση Β΄.16. Κάθε σώμα είναι ακέραια περιοχή. Το αντίστροφο εν γένει δεν ισχύει.
Απόδειξη: Έστω $(\mathrm{R}, +, \cdot)$ σώμα και $\alpha, \beta \in \mathrm{R}$ τέτοια, ώστε $\alpha\beta = 0$. Αν $\alpha \neq 0$, τότε υπάρχει το αντίστροφο α^{-1} του α με $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$. Επομένως $\alpha\beta = 0 \Rightarrow \alpha^{-1}(\alpha\beta) = \alpha^{-1} \cdot 0 = 0 \Rightarrow (\alpha^{-1}\alpha)\beta = 0 \Leftrightarrow 1 \cdot \beta = = 0 \Leftrightarrow \beta = 0$. Παρόμοια προκύπτει ότι αν $\beta \neq 0$, τότε $\alpha = 0$. Μια ακέραια περιοχή δεν είναι όμως απαραίτητα σώμα. Για παράδειγμα, το σύνολο $\mathbb{Z}$ των ακεραίων δεν είναι σώμα γιατί κάθε ακέραιος διάφορος του ± 1 δεν αντιστρέφεται στο $\mathbb{Z}$. ■

Παραδείγματα: 1) Τα σύνολα των ρητών και των πραγματικών αριθμών με τις συνηθισμένες πράξεις της πρόσθεσης και του πολλαπλασιασμού είναι σώματα. Τίθεται το ερώτημα: Υπάρχει κάποιο σώμα ανάμεσα στους ρητούς και τους πραγματικούς; Η απάντηση είναι καταφατική, όπως προκύπτει από το επόμενο παράδειγμα.
2) Γνωρίζουμε ότι ο αριθμός $\sqrt{2}$ είναι άρρητος. Θεωρούμε το σύνολο $\mathbb{Q}[\sqrt{2}] = \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}\}$. Παρατηρούμε ότι $\mathbb{Q} \subsetneq \mathbb{Q}[\sqrt{2}] \subsetneq \mathbb{R}$. Παρατηρούμε επίσης ότι αν $\alpha + \beta\sqrt{2} = 0$, τότε $\alpha = \beta = 0$. Πράγματι, έστω $\alpha + \beta\sqrt{2} = 0 \Leftrightarrow \beta\sqrt{2} = -\alpha$. Αν $\beta \neq 0$, τότε $\sqrt{2} = -\dfrac{\alpha}{\beta} \in \mathbb{Q}$, άτοπο. Άρα $\beta = 0$ και συνεπώς και $\alpha = 0$. Επίσης, αν $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Q}$, τότε $(\alpha_1 + \beta_1\sqrt{2}) \pm (\alpha_2 + \beta_2\sqrt{2}) = (\alpha_1 \pm \alpha_2) + (\beta_1 \pm \beta_2)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ και $(\alpha_1 + \beta_1\sqrt{2})(\alpha_2 + \beta_2\sqrt{2}) = (\alpha_1\alpha_2 + 2\beta_1\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Το $0 = 0 + 0\sqrt{2}$ και το $1 = 1 + 0\sqrt{2}$ είναι τα ουδέτερα στοιχεία της πρόσθεσης και του πολλαπλασιασμού αντίστοιχα. Άρα το $\mathbb{Q}[\sqrt{2}]$ είναι ένας μοναδιαίος μεταθετικός δακτύλιος (και προφανώς ακέραια περιοχή, αφού $\mathbb{Q}[\sqrt{2}] \subsetneq \mathbb{R}$). Αν τώρα $\alpha + \beta\sqrt{2} \neq 0$, όπου $\alpha, \beta \in \mathbb{Q}$, δηλαδή κάποιο από τα α, β δεν είναι μηδέν, τότε και ο αριθμός $\alpha - \beta\sqrt{2}$

δεν είναι μηδέν. Επομένως $(\alpha+\beta\sqrt{2})(\alpha-\beta\sqrt{2})=\alpha^2-2\beta^2\neq 0$. Προφανώς $\dfrac{\alpha}{\alpha^2-2\beta^2}-\dfrac{\beta}{\alpha^2-2\beta^2}\sqrt{2}\in\mathbb{Q}[\sqrt{2}]$. Αλλά $(\alpha+\beta\sqrt{2})\left(\dfrac{\alpha}{\alpha^2-2\beta^2}-\dfrac{\beta}{\alpha^2-2\beta^2}\sqrt{2}\right)=(\alpha+\beta\sqrt{2})\dfrac{\alpha-\beta\sqrt{2}}{(\alpha+\beta\sqrt{2})(\alpha-\beta\sqrt{2})}=1$, δηλαδή $(\alpha+\beta\sqrt{2})^{-1}=\dfrac{\alpha}{\alpha-2\beta^2}-\dfrac{\beta}{\alpha^2-2\beta^2}\sqrt{2}\in\mathbb{Q}[\sqrt{2}]$.

Γενικά, υπάρχουν άπειρα σώματα μεταξύ του $\mathbb{Q}$ και του $\mathbb{R}$. Όπως προκύπτει από τη θεωρία αριθμών, αν n είναι θετικός ακέραιος, ο οποίος δεν είναι τέλειο τετράγωνο ακεραίου, τότε $\sqrt{n}\notin\mathbb{Q}$. Με παρόμοιες μεθόδους προκύπτει ότι το σύνολο $\mathbb{Q}[\sqrt{n}]=\{\alpha+\beta\sqrt{n}\mid\alpha,\beta\in\mathbb{Q}\}$ είναι σώμα που περιέχεται γνήσια στο $\mathbb{R}$ και περιέχει γνήσια το $\mathbb{Q}$.

3) Εύκολα μπορεί να ελέγξει κανείς ότι το $\mathbb{Z}_2=\{\langle 0\rangle,\langle 1\rangle\}$ με τις πράξεις $+$ και $\cdot$ που περιγράψαμε στους αντίστοιχους πίνακες, είναι σώμα. Γνωρίζουμε ήδη ότι είναι ακέραια περιοχή. Αυτό δεν είναι τυχαίο, όπως αποδεικνύεται στην επόμενη πρόταση:

Πρόταση Β΄.17. Κάθε πεπερασμένη ακέραια περιοχή R είναι σώμα.

Απόδειξη: Υποθέτουμε ότι $\mathrm{R}=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$, όπου n θετικός ακέραιος. Έστω $\alpha=\alpha_i\in\mathrm{R}$, για κάποιο $i\in\{1,2,\ldots,n\}$ με $\alpha\neq 0$. Ορίζουμε την απεικόνιση $\mathrm{T}_\alpha:\mathrm{R}\to\mathrm{R}$ με $\mathrm{T}_\alpha(\alpha_j)=\alpha\alpha_j$, για κάθε $j=1,2,\ldots,n$. Παρατηρούμε ότι αν $\mathrm{T}_\alpha(\alpha_i)=\mathrm{T}_\alpha(\alpha_k)$, τότε $\alpha\alpha_j=\alpha\alpha_k\Leftrightarrow\alpha(\alpha_j-\alpha_k)=0$. Επειδή ο R είναι ακέραια περιοχή και $\alpha\neq 0$, θα πρέπει $\alpha_j-\alpha_k=0\Leftrightarrow\alpha_j=\alpha_k$, ήτοι $j=k$. Επομένως η απεικόνιση $\mathrm{T}_\alpha:\mathrm{R}\to\mathrm{R}$ είναι 1-1 και επειδή το R είναι πεπερασμένο, θα είναι και επί. Συνεπώς, αν $1=\alpha_t$, για κάποιο $t\in\{1,2,\ldots,n\}$, θα υπάρχει κάποιο α_j τέτοιο, ώστε $\mathrm{T}_\alpha(\alpha_j)=\alpha_t=1$, δηλαδή $\alpha\alpha_j=1$. Επομένως $\alpha_j=\alpha^{-1}$. ■

Παράρτημα Γ΄

Τὸ σύνολο $\mathbb{Z}$ τῶν ἀκεραίων ὡς ὑποσύνολο τοῦ συνόλου $\mathbb{R}$ τῶν πραγματικῶν ἀριθμῶν καὶ ἡ μαθηματικὴ ἐπαγωγὴ

Γ΄.1 «᾽Ολίγα τινὰ» περὶ τῶν ἀκεραίων καὶ ἡ μαθηματικὴ ἐπαγωγὴ

Στο εισαγωγικό αυτό κεφάλαιο ορίζουμε το σύνολο $\mathbb{Z}$ των ακεραίων ως υποσύνολο του $\mathbb{R}$, δεχόμενοι τα βασικά αξιώματα των πραγματικών αριθμών, όπως αυτά έχουν διδαχθεί στο μάθημα του Απειροστικού Λογισμού. Μια άλλη προσέγγιση θα ήταν να ορίσουμε τους ακεραίους και στη συνέχεια τους ρητούς και τους πραγματικούς, ξεκινώντας από το σύνολο $\mathbb{N}$ των φυσικών αριθμών και χρησιμοποιώντας τα αξιώματα του Peano. Αυτή η τελευταία προσέγγιση είναι και η πιο φυσιολογική. Επειδή όμως συνηθίζεται στα μαθήματα του Απειροστικού Λογισμού να ορίζονται πρώτα οι πραγματικοί αριθμοί, ως ένα γραμμικά διατεγμένο σώμα, το οποίο πληροί το αξίωμα της συνέχειας και επίσης για λόγους εξοικονόμησης χρόνου, θα ακολουθήσουμε την πρώτη προσέγγιση.
Υπενθυμίζουμε ότι αν $\mathcal{A} \subseteq \mathcal{P}(\Omega)$ είναι μια συλλογή (σύνολο) υποσυνόλων ενός βασικού συνόλου Ω, τότε με $\bigcap_{A\in\mathcal{A}} A$ συμβολίζουμε **την τομή όλων των συνόλων της συλλογής** $\mathcal{A}$.

Ορισμός Γ΄.1. Έστω $\mathcal{A} \subseteq \mathcal{P}(\mathbb{R})$ το σύνολο όλων των υποσυνόλων A του $\mathbb{R}$ με τις εξής ιδιότητες:
(i) $0 \in A$ και **(ii)** Για κάθε $n \in A$, ο αριθμός $n+1$ ανήκει επίσης στο A.
Θέτουμε $\mathbb{N} = \bigcap_{A\in\mathcal{A}} A$. Το σύνολο $\mathbb{N}$ ονομάζεται **σύνολο των φυσικών αριθμών**.

Παρατηρούμε ότι $[0,+\infty) \in \mathcal{A}$ και επομένως η συλλογή $\mathcal{A}$ είναι μη κενή. Επιπροσθέτως, $0 \in A$, αλλά και $1 = 0+1 \in A$, για κάθε $A \in \mathcal{A}$. Επομένως $0, 1 \in \mathbb{N} = \bigcap_{A\in\mathcal{A}} A$, ήτοι το $\mathbb{N}$ είναι μη κενό. Επειδή δε $[0,+\infty) \in \mathcal{A}$, έχουμε $\mathbb{N} = \bigcap_{A\in\mathcal{A}} A \subseteq [0,+\infty)$, ήτοι $n \geq 0$, για κάθε $n \in \mathbb{N}$. Από τον ορισμό του $\mathbb{N}$ προκύπτει η επόμενη πρόταση:

Πρόταση Γ΄.2. (Αρχή της Μαθηματικής Επαγωγής) Έστω $\mathbb{N}' \subseteq \mathbb{N}$ με τις ακόλουθες ιδιότητες:
(i) $0 \in \mathbb{N}'$ και **(ii)** $n+1 \in \mathbb{N}'$, για κάθε $n \in \mathbb{N}'$.
Τότε $\mathbb{N}' = \mathbb{N}$.
Απόδειξη: Από τον ορισμό της συλλογής $\mathcal{A}$ προκύπτει ότι $\mathbb{N}' \in \mathcal{A}$. Επομένως $\mathbb{N}' \supseteq \bigcap_{A\in\mathcal{A}} A = \mathbb{N}$. Επειδή δε $\mathbb{N}' \subseteq \mathbb{N}$, έπεται ότι $\mathbb{N}' = \mathbb{N}$. ■

Ο αριθμός $n+1$ λέγεται **επόμενος** του n και ο αριθμός $n-1$ λέγεται **προηγούμενος** του n. Από τον ορισμό του $\mathbb{N}$ προκύπτει ότι ο επόμενος ενός φυσικού αριθμού είναι φυσικός.

Πρόταση Γ΄.3. Αν $n > 0$ είναι φυσικός αριθμός, τότε και ο προηγούμενός του $n-1$ είναι φυσικός αριθμός.
Απόδειξη: Υποθέτουμε ότι η πρόταση δεν είναι αληθής. Τότε υπάρχει $n_0 \in \mathbb{N}$, με $n_0 > 0$ τέτοιος, ώστε $n_0 - 1 \notin \mathbb{N}$. Θεωρούμε το σύνολο $\mathbb{N}' = \mathbb{N} \setminus \{n_0\}$. Παρατηρούμε ότι $0 \in \mathbb{N}'$, εφόσον $n_0 > 0$.
Έστω τώρα $n \in \mathbb{N}' \subseteq \mathbb{N}$. Αν $n+1 = n_0$, τότε $n = n_0 - 1 \notin \mathbb{N}$, σύμφωνα με την υπόθεση. Αυτό όμως είναι

ἄτοπο γιατί $n \in \mathbb{N}$. Ἄρα $n+1 \neq n_0$, δηλαδή $n+1 \in \mathbb{N} \setminus \{n_0\} = \mathbb{N}'$. Με βάση την προηγούμενη πρόταση παίρνουμε $\mathbb{N}' = \mathbb{N} \setminus \{n_0\} = \mathbb{N}$, που σημαίνει ότι $n_0 \notin \mathbb{N}$, ἄτοπο. ■

Πρόταση Γ΄.4. Ανάμεσα σε δύο διαδοχικούς φυσικούς δεν υπάρχει φυσικός, δηλαδή αν $n \in \mathbb{N}$, τότε δεν υπάρχει $k \in \mathbb{N}$ με $n < k < n+1$.
Απόδειξη: Έστω $\mathbb{N}' = \{n \in \mathbb{N} |\ \nexists\, k \in \mathbb{N}$ με $n < k < n+1\}$. Παρατηρούμε ότι $0 \in \mathbb{N}'$ γιατί, αν $0 < k < 1$ για κάποιο $k \in \mathbb{N}$, τότε με βάση την προηγούμενη πρόταση, εφόσον $0 < k$, ο προηγούμενος $k-1$ του k ανήκει στο $\mathbb{N}$. Αλλά $k - 1 < 0$, ἄτοπο γιατί $\mathbb{N} \subseteq [0, +\infty)$.
Υποθέτουμε ότι $n \in \mathbb{N}'$. Αν $n+1 \notin \mathbb{N}'$, τότε θα υπήρχε $k \in \mathbb{N}$ με $n+1 < k < n+2$. Εφόσον $0 \leq n < n+1 < k$, ο $k-1$ ανήκει στο $\mathbb{N}$ και μάλιστα $n < k-1 < n+1$, δηλαδή $n \notin \mathbb{N}'$, ἄτοπο. Ἄρα $n+1 \in \mathbb{N}'$ και επομένως $\mathbb{N}' = \mathbb{N}$. ■

Πρόταση Γ΄.5. Το σύνολο των φυσικών είναι κλειστό ως προς την πρόσθεση και τον πολλαπλασιασμό, δηλαδή αν $m, n \in \mathbb{N}$, τότε $m+n, mn \in \mathbb{N}$.
Απόδειξη: Έστω $m \in \mathbb{N}$. Όπως προηγουμένως, θέτουμε $\mathbb{N}' = \{n \in \mathbb{N} |\ m+n \in \mathbb{N}\}$. Εφόσον $m+0 = m \in \in \mathbb{N}$, έχουμε $0 \in \mathbb{N}'$. Έστω $n \in \mathbb{N}'$, ήτοι $m+n \in \mathbb{N}$. Τότε $m+(n+1) = (m+n)+1 \in \mathbb{N}$, ως ο επόμενος του φυσικού αριθμού $m+n$. Επομένως $n+1 \in \mathbb{N}'$. Συμπεραίνουμε λοιπόν ότι $\mathbb{N}' = \mathbb{N}$ και κατά συνέπεια, εφόσον ο m είναι τυχόν φυσικός, $m+n \in \mathbb{N}$, για κάθε $m, n \in \mathbb{N}$.
Για τον πολλαπλασιασμό εφαρμόζουμε την ίδια μέθοδο της μαθηματικής επαγωγής. Έστω $m \in \mathbb{N}$. Θεωρούμε το σύνολο $\mathbb{N}'' = \{n \in \mathbb{N} |\ mn \in \mathbb{N}\}$. Έχουμε $m \cdot 0 = 0 \in \mathbb{N}$ και συνεπώς $0 \in \mathbb{N}''$. Έστω τώρα ότι $n \in \mathbb{N}''$, δηλαδή $mn \in \mathbb{N}$. Τότε $m(n+1) = mn + m$. Από υπόθεση $mn \in \mathbb{N}$. Επίσης δείξαμε προηγουμένως ότι το $\mathbb{N}$ είναι κλειστό ως προς την πρόσθεση. Ἄρα $m(n+1) = mn + m \in \mathbb{N}$. Συνεπώς και $n+1 \in \mathbb{N}''$. Συμπεραίνουμε λοιπόν ότι $\mathbb{N}'' = \mathbb{N}$ και τελειώσαμε. ■

Πρόταση Γ΄.6. Έστω $m, n \in \mathbb{N}$ με $m \leq n$. Τότε $n - m \in \mathbb{N}$. Ιδιαιτέρως, αν $m < n$, τότε $n - m \geq 1$.
Απόδειξη: Έστω $\mathbb{N}' = \{n \in \mathbb{N} |$ με $n - m \in \mathbb{N}\ \forall\, m \in \mathbb{N}$ με $m \leq n\}$. Το μηδέν είναι προφανώς το ελάχιστο στοιχείο του $\mathbb{N}$ και άρα, αν $m \in \mathbb{N}$ με $m \leq 0$, τότε $m = 0$, οπότε $0 - m = 0 - 0 = 0 \in \mathbb{N}$. Ἄρα $0 \in \mathbb{N}'$.
Έστω τώρα $n \in \mathbb{N}'$, δηλαδή $n - m \in \mathbb{N}$, για κάθε $m \in \mathbb{N}$ με $m \leq n$. Θεωρούμε τώρα τον φυσικό $n+1$ και $m \in \mathbb{N}$ με $m \leq n+1$. Αν $m = n+1$, τότε $n+1-m = n+1-(n+1)0 \in \mathbb{N}$. Έστω $m < n+1$. Επειδή, όπως αποδείξαμε προηγουμένως, δεν υπάρχει φυσικός στο διάστημα $(n, n+1)$, θα πρέπει $m \leq n$. Από την υπόθεση για τον n προκύπτει ότι ο αριθμός $k = n - m$ είναι φυσικός. Ἄρα $n+1-m = k+1 \in \mathbb{N}$. Συμπεραίνουμε λοιπόν ότι $n+1 \in \mathbb{N}$. Τελικώς, $\mathbb{N}' = \mathbb{N}$. Ἄρα $n - m \in \mathbb{N}$, για κάθε $m, n \in \mathbb{N}$ με $m \leq n$. Ιδιαιτέρως, αν $m < n$, τότε επειδή δεν υπάρχει θετικός φυσικός στο διάστημα $(0, 1)$, θα πρέπει $n - m \geq 1$ και η απόδειξη θεωρείται πλήρης. ■

Ορισμός Γ΄.7. Θέτουμε $\mathbb{Z}_+ = \{1, 2, 3 \ldots\} = \{n \in \mathbb{N} |\ n > 0\}$ για το σύνολο των θετικών φυσικών αριθμών. Τα στοιχεία του $\mathbb{Z}_+$ ονομάζονται **θετικοί ακέραιοι**. Επίσης θέτουμε $\mathbb{Z}_- = -\mathbb{Z}_+ = \{\ldots, -3, -2, -1\}$. Τα στοιχεία του $\mathbb{Z}_-$ ονομάζονται **αρνητικοί ακέραιοι**. Το σύνολο $\mathbb{Z} = \mathbb{Z}_- \cup \{0\} \cup \mathbb{Z}_+$ ονομάζεται **σύνολο των ακεραίων αριθμών** και τα στοιχεία του **ακέραιοι αριθμοί**.

Πρόταση Γ΄.8. Το σύνολο $\mathbb{Z}$ είναι κλειστό ως προς την πρόσθεση, τον πολλαπλασιασμό και την αφαίρεση.
Απόδειξη: Κατ' αρχάς παρατηρούμε ότι για κάθε ακέραιο n ισχύει: $|n| = \begin{cases} n, & \text{αν } n \geq 0 \\ -n, & \text{αν } n < 0 \end{cases}$, δηλαδή $|n| = n \Leftrightarrow n \in \mathbb{N}$ και αν $n \in \mathbb{Z}_-$, τότε $|n| = -n \in \mathbb{Z}_+ \subseteq \mathbb{N}$.
Έστω τώρα $m, n \in \mathbb{Z}$. Όσον αφορά το άθροισμα $m+n$, διακρίνουμε περιπτώσεις:
(i) Κάποιος από τους m, n είναι μηδέν. Τότε το άθροισμά τους θα είναι $m \in \mathbb{Z}$ ή $n \in \mathbb{Z}$.
(ii) $m, n \in \mathbb{N}$, δηλαδή και οι δύο μη αρνητικοί ακέραιοι. Επειδή το $\mathbb{N}$ είναι κλειστό ως προς την πρόσθεση, θα έχουμε $m+n \in \mathbb{N} \subseteq \mathbb{Z}$.
(iii) $m, n \in \mathbb{Z}_-$. Τότε $-m, -n \in \mathbb{Z}_+$ και επομένως $-(m+n) = (-m)+(-n) \in \mathbb{Z}_+$. Ἄρα $m+n \in -\mathbb{Z}_+ = = \mathbb{Z}_- \subseteq \mathbb{Z}$.
(iv) Ο ένας είναι αρνητικός και ο άλλος θετικός. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $m \in \mathbb{Z}_-$ και $n \in \mathbb{Z}_+$. Τότε $k := |m| = -m \in \mathbb{Z}_+ \subseteq \mathbb{N}$, ήτοι $m = -k$. Αν $k \leq n$, τότε από

την προηγούμενη πρόταση προκύπτει ότι $n+m = n-k \in \mathbb{N} \subseteq \mathbb{Z}$. Αν $k > n$, τότε πάλι από την προηγούμενη πρόταση προκύπτει ότι $k-n \in \mathbb{N}$ και επειδή $k-n > 0$, έχουμε $k-n \in \mathbb{Z}_+$. Άρα $m+n = -k+n = -(k-n) \in -\mathbb{Z}_+ = \mathbb{Z}_- \subseteq \mathbb{Z}$.
Για τον πολλαπλασιασμό διακρίνουμε πάλι περιπτώσεις:
(i)΄ Κάποιος από τους δύο είναι μηδέν. Τότε το γινόμενό τους είναι $0 \in \mathbb{Z}$.
(ii)΄ $m, n \in \mathbb{N}$. Τότε και $mn \in \mathbb{N} \subseteq \mathbb{Z}$.
(iii)΄ $m, n \in \mathbb{Z}_-$. Τότε $-m, -n \in \mathbb{Z}_+$. Άρα $mn = (-m)(-n) \in \mathbb{Z}_+ \subseteq \mathbb{Z}$.
(iv)΄ Ο ένας είναι αρνητικός και ο άλλος θετικός. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $m \in \mathbb{Z}_-$ και $n \in \mathbb{Z}_+$. Τότε $-m \in \mathbb{Z}_+$ και άρα $-(mn) = (-m)n \in \mathbb{Z}_+$. Επομένως $mn \in -\mathbb{Z}_+ = \mathbb{Z}_- \subseteq \mathbb{Z}$.
Τώρα, όσον αφορά την αφαίρεση, έστω $m, n \in \mathbb{Z}$. Επειδή $-1 \in \mathbb{Z}$ και λόγω της κλειστότητας του $\mathbb{Z}$ ως προς τον πολλαπλασιασμό, έχουμε $-m = (-1)m \in \mathbb{Z}$. Λόγω δε της κλειστότητας του $\mathbb{Z}$ ως προς την πρόσθεση, $n-m = n+(-m) \in \mathbb{Z}$. ■

Πόρισμα Γ΄.9. Το σύνολο $\mathbb{Z}$ εφοδιασμένο με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού που κληρονομεί από το σύνολο των πραγματικών $\mathbb{R}$ είναι ακέραια περιοχή. ■

Ορισμός Γ΄.10. Δύο ή περισσότεροι ακέραιοι της μορφής $m, m+1, m+2, \ldots$ λέγονται **διαδοχικοί**.

Πόρισμα Γ΄.11. (i) Δεν υπάρχει ακέραιος μεταξύ δύο διαδοχικών ακεραίων.
(ii) Έστω $m, n \in \mathbb{Z}$ με $m \leq n$. Τότε $n-m \in \mathbb{N}$. Ιδιαιτέρως, αν $m < n$, τότε $n-m \geq 1$, δηλαδή $n-m \in \mathbb{Z}_+$.
Απόδειξη: (i) Έστω $n, k \in \mathbb{Z}$ με $n < k < n+1$. Τότε $0 < k-n < 1$, δηλαδή το $k-n$ είναι θετικός ακέραιος, άρα θετικός φυσικός που ανήκει στο διάστημα $(0,1)$. Αυτό όμως αντιβαίνει στην πρόταση Γ.4.
(ii) Ο ακέραιος $n-m$ είναι μη αρνητικός, άρα φυσικός. Επίσης, αν $m < n$, τότε ο $n-m$ είναι θετικός φυσικός και άρα, με βάση την πρόταση Γ.4 δεν ανήκει στο διάστημα $(0,1)$. Άρα, είναι μεγαλύτερος ή ίσος του 1. ■

Πρόταση Γ΄.12. Το σύνολο $\mathbb{Z}$ δεν είναι ούτε άνω ούτε κάτω φραγμένο στο $\mathbb{R}$.
Απόδειξη: Υποθέτουμε ότι το $\mathbb{Z}$ είναι άνω φραγμένο και $s = \sup \mathbb{Z}$. Τότε το $s - \frac{1}{2}$ δεν είναι άνω φράγμα του $\mathbb{Z}$. Άρα υπάρχει $m \in \mathbb{Z}$ τέτοιος, ώστε $s - \frac{1}{2} < m$. Αλλά, τότε $s < s + \frac{1}{2} < m+1 \in \mathbb{Z}$, άτοπο γιατί το s είναι άνω φράγμα του $\mathbb{Z}$.
Ομοίως, αν το $\mathbb{Z}$ είναι κάτω φραγμένο και $t = \inf \mathbb{Z}$, τότε το $t + \frac{1}{2}$ δεν είναι κάτω φράγμα του $\mathbb{Z}$. Άρα υπάρχει $m \in \mathbb{Z}$ τέτοιο, ώστε $m < t + \frac{1}{2}$. Συνεπώς $m-1 < t - \frac{1}{2} < t$ και $m-1 \in \mathbb{Z}$, άτοπο. ■

Πόρισμα Γ΄.13. Κάθε μη κενό και κάτω φραγμένο υποσύνολο Α του $\mathbb{Z}$ έχει ελάχιστο στοιχείο. Ομοίως, κάθε μη κενό και άνω φραγμένο υποσύνολο Β του $\mathbb{Z}$ έχει μέγιστο στοιχείο.
Απόδειξη: Έστω $\varnothing \neq \mathrm{A} \subseteq \mathbb{Z}$, με Α κάτω φραγμένο. Έστω $t = \inf \mathrm{A}$. Τότε υπάρχει $m \in \mathrm{A}$ με $m < t + \frac{1}{2}$. Αν το m δεν ήταν το ελάχιστο στοιχείο του Α, θα υπήρχε $m' \in \mathrm{A}$ με $m' < m$. Συνεπώς $t \leq m' < m < t + \frac{1}{2}$ και κατά συνέπεια $m - m' < \frac{1}{2}$. Αυτό όμως αντιβαίνει στο πόρισμα Γ.11(ii).
Ομοίως, έστω $\varnothing \neq \mathrm{A} \subseteq \mathbb{Z}$, με Α άνω φραγμένο. Έστω $s = \sup \mathrm{A}$. Τότε υπάρχει $m \in \mathrm{A}$, με $m > s - \frac{1}{2}$. Αν το m δεν ήταν το μέγιστο στοιχείο του Α, θα υπήρχε $m' \in \mathrm{A}$ με $s - \frac{1}{2} < m < m' \leq s$. Συνεπώς $m' - m < \frac{1}{2}$, που και αυτό αντιβαίνει στο πόρισμα Γ.11(ii). ■

Ορισμός Γ΄.14. Έστω $x \in \mathbb{R}$. Εφόσον το $\mathbb{Z}$ δεν είναι ούτε κάτω και ούτε άνω φραγμένο, τα σύνολα $\mathbb{Z}_{\leq x} = \{n \in \mathbb{Z} |\ n \leq x\}$ και $\mathbb{Z}_{\geq x} = \{n \in \mathbb{Z} |\ n \geq x\}$ είναι μη κενά. Το $\mathbb{Z}_{\leq x}$ είναι άνω φραγμένο από το x, άρα έχει μέγιστο στοιχείο. Το στοιχείο αυτό συμβολίζεται με $\lfloor x \rfloor$ και ονομάζεται **ακέραιο μέρος του x**. Επίσης, το $\mathbb{Z}_{\geq x}$ είναι κάτω φραγμένο από το x και συνεπώς έχει ελάχιστο στοιχείο. Το στοιχείο αυτό συμβολίζεται με $\lceil x \rceil$ και ονομάζεται **ακέραια οροφή του x**.

Από τον προηγούμενο ορισμό προκύπτει το επόμενο πόρισμα:

Πόρισμα Γ΄.15. Έστω $x \in \mathbb{R}$. Τότε ισχύουν οι σχέσεις: **(i)** $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ και **(ii)** $\lceil x \rceil - 1 < x \leq \lceil x \rceil$. Αντιστρόφως, αν $k \in \mathbb{Z}$ με $k \leq x < k+1$, τότε $k = \lfloor x \rfloor$. Επίσης, αν $r \in \mathbb{Z}$ με $r - 1 < x \leq r$, τότε $r = \lceil x \rceil$. Προφανώς ισχύει η ισοδυναμία: $x \in \mathbb{Z} \Leftrightarrow \lfloor x \rfloor = \lceil x \rceil$.
Απόδειξη: Οι σχέσεις **(i)** και **(ii)** προκύπτουν άμεσα από τον προηγούμενο ορισμό. Έστω τώρα $k \in \mathbb{Z}$ με $k \leq x < k+1$. Προφανώς $k \in \mathbb{Z}_{\leq x}$. Επειδή $x < k+1$, ο k είναι αναγκαστικά το $\max \mathbb{Z}_{\leq x} = \lfloor x \rfloor$.
Ομοίως, αν $r - 1 < x \leq r$, ο ακέραιος $r \in \mathbb{Z}_{\geq x}$ ισούται αναγκαστικά με $\min \mathbb{Z}_{\geq x} = \lceil x \rceil$. ■

Συμβολισμός: Συμβολίζουμε με $\{x\}$ τη διαφορά $x - \lfloor x \rfloor \in [0, 1)$.

ΛΥΜΕΝΕΣ ΑΣΚΗΣΕΙΣ

Άσκηση 100. Αν $k \in \mathbb{Z}$ και $x \in \mathbb{R}$, τότε $\lfloor x + k \rfloor = \lfloor x \rfloor + k$ και $\lceil x + k \rceil = \lceil x \rceil + k$.
Απόδειξη: Εξ ορισμού $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. Επομένως $\lfloor x \rfloor + k \leq x + k < (\lfloor x \rfloor + k) + 1$. Με βάση το προηγούμενο πόρισμα, $\lfloor x \rfloor + k = \lfloor x + k \rfloor$. Με παρόμοιο τρόπο αποδεικνέται ότι $\lceil x + k \rceil = \lceil x \rceil + k$. ■

Άσκηση 101. Δείξτε ότι για κάθε $x, y \in \mathbb{R}$ ισχύει η σχέση: $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
Απόδειξη: Από τις σχέσεις $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ και $\lfloor y \rfloor \leq y < \lfloor y \rfloor + 1$ προκύπτει ότι $\lfloor x \rfloor + \lfloor y \rfloor \leq$ $\leq x + y < \lfloor x \rfloor + \lfloor y \rfloor + 2$. Επειδή ο $\lfloor x + y \rfloor$ είναι ο μέγιστος ακέραιος που δεν υπερβαίνει το $x + y$, έχουμε $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$. Αλλά $\lfloor x + y \rfloor \leq x + y < \lfloor x \rfloor + \lfloor y \rfloor + 2$. Άρα $\lfloor x + y \rfloor < \lfloor x \rfloor + \lfloor y \rfloor + 2$ και κατά συνέπεια $\lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 2 - 1 = \lfloor x \rfloor + \lfloor y \rfloor + 1$. ■

Άσκηση 102. Έστω $x \in \mathbb{R}$ και n θετικός ακέραιος. Τότε $\left\lfloor \dfrac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \dfrac{x}{n} \right\rfloor$.

Απόδειξη: Έχουμε: $\lfloor x \rfloor \leq x \Leftrightarrow \dfrac{\lfloor x \rfloor}{n} \leq \dfrac{x}{n} \Rightarrow \left\lfloor \dfrac{\lfloor x \rfloor}{n} \right\rfloor \leq \left\lfloor \dfrac{x}{n} \right\rfloor$.
Επίσης $\left\lfloor \dfrac{x}{n} \right\rfloor \leq \dfrac{x}{n} \Rightarrow n\left\lfloor \dfrac{x}{n} \right\rfloor \leq x$. Επειδή $n\left\lfloor \dfrac{x}{n} \right\rfloor \in \mathbb{Z}$ και το $\lfloor x \rfloor$ είναι ο μεγαλύτερος ακέραιος που δεν υπερβαίνει τον x, θα έχουμε $n\left\lfloor \dfrac{x}{n} \right\rfloor \leq \lfloor x \rfloor \Rightarrow \left\lfloor \dfrac{x}{n} \right\rfloor \leq \dfrac{\lfloor x \rfloor}{n}$. Αλλά ο $\left\lfloor \dfrac{\lfloor x \rfloor}{n} \right\rfloor$ είναι ο μεγαλύτερος ακέραιος που δεν υπερβαίνει τον $\dfrac{\lfloor x \rfloor}{n}$. Επομένως $\left\lfloor \dfrac{x}{n} \right\rfloor \leq \left\lfloor \dfrac{\lfloor x \rfloor}{n} \right\rfloor$. ■

Άσκηση 103. (Ταυτότητα του Hermite) Έστω $x \in \mathbb{R}$ και n θετικός ακέραιος. Τότε

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor.$$

Απόδειξη: Θεωρούμε τη συνάρτηση $f(x) = \lfloor x \rfloor + \left\lfloor x + \dfrac{1}{n} \right\rfloor + \left\lfloor x + \dfrac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \dfrac{n-1}{n} \right\rfloor - \lfloor nx \rfloor$, $x \in \mathbb{R}$.
Αν $x \in \left[0, \dfrac{1}{n}\right)$, τότε για κάθε $k = 0, 1, 2, \ldots, n-1$, έχουμε $0 \leq x + \dfrac{k}{n} < \dfrac{k+1}{n} \leq \dfrac{n-1+1}{n} = 1$. Άρα $\left\lfloor x + \dfrac{k}{n} \right\rfloor = 0$, για κάθε $k = 0, 1, 2, \ldots, n-1$. Επίσης, $0 \leq nx < n \cdot \dfrac{1}{n} = 1$. Άρα και $\lfloor nx \rfloor = 0$. Επομένως $f(x) = 0$, για κάθε $x \in \left[0, \dfrac{1}{n}\right)$.
Τώρα $f\left(x + \dfrac{1}{n}\right) = \left\lfloor x + \dfrac{1}{n} \right\rfloor + \left\lfloor x + \dfrac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \dfrac{n-1}{n} \right\rfloor + \left\lfloor x + \dfrac{n}{n} \right\rfloor - \left\lfloor n\left(x + \dfrac{1}{n}\right) \right\rfloor = \left\lfloor x + \dfrac{1}{n} \right\rfloor + \left\lfloor x + \dfrac{2}{n} \right\rfloor +$
$+ \cdots + \left\lfloor x + \dfrac{n-1}{n} \right\rfloor + \lfloor x + 1 \rfloor - \lfloor nx + 1 \rfloor \underset{\text{Άσκηση Γ.1}}{=} \lfloor x \rfloor + 1 + \left\lfloor x + \dfrac{1}{n} \right\rfloor + \left\lfloor x + \dfrac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \dfrac{n-1}{n} \right\rfloor - \lfloor nx \rfloor - 1 =$
$= \lfloor x \rfloor + \left\lfloor x + \dfrac{1}{n} \right\rfloor + \left\lfloor x + \dfrac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \dfrac{n-1}{n} \right\rfloor - \lfloor nx \rfloor = f(x)$, για κάθε $x \in \mathbb{R}$. Άρα η συνάρτηση f είναι περιοδική με περίοδο $\dfrac{1}{n}$. Επειδή λοιπόν μηδενίζεται στο διάστημα $\left[0, \dfrac{1}{n}\right)$, θα μηδενίζεται παντού. Η απόδειξη είναι πλήρης. ■

Άσκηση 104. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύει η σχέση

$$\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{8} \right\rfloor + \left\lfloor \frac{n+8}{16} \right\rfloor + \cdots = n.$$

Απόδειξη: Παρατηρούμε ότι $\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{8} \right\rfloor + \left\lfloor \frac{n+8}{16} \right\rfloor + \cdots = \left\lfloor \frac{n}{2} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{n}{4} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{n}{8} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{n}{16} + \frac{1}{2} \right\rfloor + \cdots = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} + \frac{1}{2} \right\rfloor$. Το τελευταίο άθροισμα είναι όμως πεπερασμένο, καθώς οι όροι του από ένα σημείο και πέρα μηδενίζονται. Πράγματι, αφού $\lim\limits_{k \to +\infty} \frac{n}{2^k} = 0$, θα υπάρχει θετικός ακέραιος k_0 τέτοιος, ώστε $\frac{n}{2^k} < \frac{1}{2}$, για κάθε $k \geq k_0$. Τότε όμως $\frac{n}{2^k} + \frac{1}{2} < 1$ και επομένως $\left\lfloor \frac{n}{2^k} + \frac{1}{2} \right\rfloor = 0$. Χρησιμοποιούμε την πιο απλή μορφή της ταυτότητας του Hermite: $\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor$. Έχουμε τις ακόλουθες σχέσεις:

$$\begin{aligned}
\cancel{\left\lfloor \frac{n}{2} \right\rfloor} + \left\lfloor \frac{n}{2} + \frac{1}{2} \right\rfloor &= \left\lfloor 2 \cdot \frac{n}{2} \right\rfloor = n \\
\cancel{\left\lfloor \frac{n}{4} \right\rfloor} + \left\lfloor \frac{n}{4} + \frac{1}{2} \right\rfloor &= \left\lfloor 2 \cdot \frac{n}{4} \right\rfloor = \cancel{\left\lfloor \frac{n}{2} \right\rfloor} \\
\cancel{\left\lfloor \frac{n}{8} \right\rfloor} + \left\lfloor \frac{n}{8} + \frac{1}{2} \right\rfloor &= \left\lfloor 2 \cdot \frac{n}{8} \right\rfloor = \cancel{\left\lfloor \frac{n}{4} \right\rfloor} \\
\cancel{\left\lfloor \frac{n}{16} \right\rfloor} + \left\lfloor \frac{n}{16} + \frac{1}{2} \right\rfloor &= \left\lfloor 2 \cdot \frac{n}{16} \right\rfloor = \cancel{\left\lfloor \frac{n}{8} \right\rfloor} \\
\cancel{\left\lfloor \frac{n}{32} \right\rfloor} + \left\lfloor \frac{n}{32} + \frac{1}{2} \right\rfloor &= \left\lfloor 2 \cdot \frac{n}{32} \right\rfloor = \cancel{\left\lfloor \frac{n}{16} \right\rfloor} \\
&\vdots
\end{aligned}$$

Προσθέτοντας κατά μέλη και διαγράφοντας τους ίσους όρους, όπως φαίνεται παραπάνω, παίρνουμε

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} + \frac{1}{2} \right\rfloor = n$$

■

Μπορούμε τώρα να γενικεύσουμε την αρχή της μαθηματικής επαγωγής στο σύνολο των ακεραίων. Θα δώσουμε διάφορες παραλλαγές αυτής, χρήσιμες για τις εφαρμογές.

Πρόταση Γ΄.16. Έστω $n_0 \in \mathbb{Z}$. Θεωρούμε τα σύνολα $\mathbb{Z}_{\geq n_0} = \{n \in \mathbb{Z} |\ n \geq n_0\}$ και $\mathbb{Z}_{\leq n_0} = \{n \in \in \mathbb{Z} |\ n \leq n_0\}$. Τότε ισχύουν τα εξής:
(i) Έστω $\mathrm{A} \subseteq \mathbb{Z}_{\geq n_0}$ με τις ιδιότητες:
α) $n_0 \in \mathrm{A}$ και **β)** για κάθε $n \in \mathbb{Z}$ ισχύει η συνεπαγωγή: $n \in \mathrm{A} \Rightarrow n+1 \in \mathrm{A}$. Τότε $\mathrm{A} = \mathbb{Z}_{\geq n_0}$.
(ii) Έστω $\mathrm{A} \subseteq \mathbb{Z}_{\leq n_0}$ με τις ιδιότητες:
α) $n_0 \in \mathrm{A}$ και **β)** για κάθε $n \in \mathbb{Z}$ ισχύει η συνεπαγωγή: $n \in \mathrm{A} \Rightarrow n-1 \in \mathrm{A}$. Τότε $\mathrm{A} = \mathbb{Z}_{\leq n_0}$.
Απόδειξη: (i) Έστω ότι $\mathrm{A} \subsetneq \mathbb{Z}_{\geq n_0}$. Τότε το σύνολο $\mathrm{A}' = \mathbb{Z}_{n \geq n_0} \setminus \mathrm{A}$ είναι μη κενό και κάτω φραγμένο (από το n_0). Συνεπώς έχει ένα ελάχιστο στοιχείο $m > n_0$ (γιατί $n_0 \in \mathrm{A}$). Με βάση το πόρισμα Γ΄.11(ii), $m - n_0 \geq 1$ και επομένως $m - 1 \geq n_0$. Άρα $m - 1 \in \mathbb{Z}_{\geq n_0}$. Εφόσον το m είναι το ελάχιστο στοιχείο του A', το $m-1$ δεν ανήκει στο A', δηλαδή $m - 1 \in \mathrm{A}$. Αλλά, λόγω της υπόθεσης β), $m = (m-1) + 1 \in \mathrm{A}$, άτοπο.
(ii) Η απόδειξη είναι παρόμοια με αυτήν του **(i)** γιατί, στην περίπτωση που $\mathrm{A} \subsetneq \mathbb{Z}_{\leq n_0}$, το $\mathrm{A}' = \mathbb{Z}_{\leq n_0} \setminus \mathrm{A}$ είναι άνω φραγμένο (από το n_0) υποσύνολο του $\mathbb{Z}_{\leq n_0}$. Μετά προχωρούμε συμμετρικά. ■

Η προηγούμενη πρόταση χρησιμοποιείται στην απόδειξη ιδιοτήτων οι οποίες αναφέρονται στους ακεραίους (με άμεσο ή έμμεσο τρόπο). Ας αποδείξουμε λοιπόν το εξής: Για κάθε θετικό ακέραιο n ισχύει ο τύπος

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

1ο βήμα: Αποδεικνύουμε ότι η πρόταση είναι αληθής για τον ελάχιστο δυνατό ακέραιο $n_0 = 1$. Πράγματι, για $n = 1$ το άθροισμα του πρώτου μέλους της αποδεικτέας σχέσης περιέχει μόνον το 1. Άρα το πρώτο

μέλος ισούται με 1.

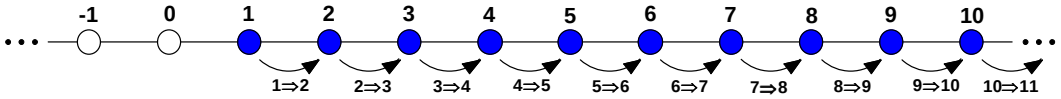
Από την άλλη μεριά, για $n=1$ το $2^{\text{ο}}$ μέλος ισούται με $\dfrac{1\cdot(1+1)}{2}=1$. Άρα για $n=1$ η πρόταση αληθεύει.

$2^{\text{ο}}$ βήμα: Υποθέτουμε τώρα ότι έχουμε αποδείξει τη σχέση $1+2+3+\cdots+n=\dfrac{n(n+1)}{2}$ για κάποιο n. Με δεδομένη τη σχέση $1+2+3+\cdots+n=\dfrac{n(n+1)}{2}$ θα αποδείξουμε ότι ισχύει η αντίστοιχη σχέση για τον επόμενο του n ακέραιο, δηλαδή τον $n+1$. Πρέπει επομένως να δείξουμε ότι $1+2+3+\cdots+n+(n+1)=\dfrac{(n+1)(n+2)}{2}$ (με την υπόθεση φυσικά ότι ισχύει η σχέση $1+2+3+\cdots+n=\dfrac{n(n+1)}{2}$).

Πράγματι, αν προσθέσουμε και στα δύο μέλη της σχέσης $1+2+3+\cdots+n=\dfrac{n(n+1)}{2}$ **(την οποία επαναλαμβάνουμε ότι θεωρούμε δεδομένη)** το $n+1$ θα πάρουμε:

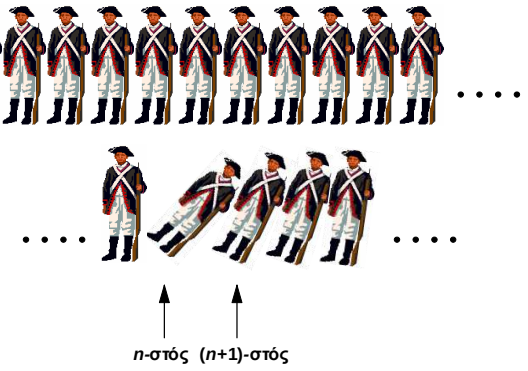
$$1+2+3+\cdots+n+(n+1)=\frac{n(n+1)}{2}+(n+1)=(n+1)\left(\frac{n}{2}+1\right)=(n+1)\frac{n+2}{2}=\frac{(n+1)(n+2)}{2}=$$
$$=\frac{(n+1)((n+1)+1)}{2}.$$

Ας δούμε τώρα τι πετύχαμε. Με βάση το $1^{\text{ο}}$ βήμα η πρόταση ισχύει για $n=1$.
Όμως, αφού ισχύει για $n=1$, τότε σύμφωνα με το $2^{\text{ο}}$ βήμα η πρόταση θα ισχύει και για $n=1+1=2$.
Αφού ισχύει για $n=2$, σύμφωνα πάλι με το $2^{\text{ο}}$ βήμα θα ισχύει και για $n=3$.
Αφού ισχύει για $n=3$, σύμφωνα πάλι με το $2^{\text{ο}}$ βήμα θα ισχύει και για $n=4$.
.....
Προφανώς αυτή η διαδικασία δεν σταματά. Μπορούμε έτσι να αποδείξουμε ότι η σχέση αυτή ισχύει π.χ. για $n=1000000$, ξεκινώντας από το $1^{\text{ο}}$ βήμα και εφαρμόζοντας το $2^{\text{ο}}$ βήμα (το οποίο ονομάζεται και **επαγωγικό βήμα**) 999999 φορές. Είναι λογικό λοιπόν να συμπεράνουμε ότι η πρόταση θα ισχύει για κάθε θετικό ακέραιο n, οσοδήποτε μεγάλος και αν είναι αυτός ο ακέραιος n. Κάποια στιγμή, ξεκινώντας από την αρχική τιμή και εφαρμόζοντας το επαγωγικό βήμα θα τον «φτάσουμε». Η παραπάνω διαδικασία αποδίδεται σχηματικά ως ακολούθως:



Σχήμα 9

Η διαδικασία αυτή θυμίζει λίγο το παιχνίδι του «ντόμινο». Σ΄ αυτό το παιχνίδι τοποθετούμε διαδοχικά διάφορα αντικείμενα (συνήθως πλάκες) κατά τέτοιο τρόπο ώστε αν πέσει κάποιο αντικείμενο, τότε αυτό θα συμπαρασύρει και το επόμενο, και το επόμενο,...κ.ο.κ. Μέχρι να πέσουν όλα.
Στο επόμενο σχήμα δεν έχουμε τοποθετήσει πλάκες αλλά στρατιωτάκια.



Σχήμα 10

Αν ρίξουμε το n-στό στρατιωτάκι αυτό θα συμπαρασύρει και το επόμενο, το $(n+1)$-στό. Αν λοιπόν ρίξουμε

π.χ. το πέμπτο, αυτό θα συμπαρασύρει όλα τα υπόλοιπα και τελικά **όλα** τα στρατιωτάκια από το 5ο και μετά θα πέσουν. (Αν δεν πέσουν όλα αυτό σημαίνει ότι κάποιο έπεσε αλλά όχι το επόμενό του, δηλαδή δεν ισχύει η συνεπαγωγή ***n*-στό ⇒ (*n*+1)-στό**.
Ας υποθέσουμε λοιπόν ότι έχουμε έναν προτασιακό τύπο $p(n)$, δηλαδή μια έκφραση η οποία γίνεται πρόταση (αληθής ή ψευδής) για ορισμένες ακέραιες τιμές της μεταβλητής n. Καλούμαστε να αποδείξουμε ότι ο προτασιακός τύπος δίνει αληθή πρόταση για κάθε ακέραιο n μεγαλύτερο ή ίσο ενός αρχικού n_0. Ακολουθούμε τα εξής βήματα:
1ο βήμα: Αποδεικνύουμε ότι η πρόταση $p(n_0)$ είναι αληθής.
2ο βήμα: Με την υπόθεση ότι η $p(n)$ είναι αληθής, αποδεικνύουμε ότι και η $p(n+1)$ είναι αληθής. (Επαγωγικό βήμα)
Η αποδεικτική αυτή διαδικασία ονομάζεται **απόδειξη με επαγωγή**. Πράγματι, εφόσον η $p(n_0)$ είναι αληθής, με βάση το 2ο βήμα, θα είναι αληθής και η $p(n_0+1)$. Και πάλι με βάση το επαγωγικό βήμα θα είναι αληθής και η $p(n_0+2)$. Μετά πάλι από την $p(n_0+2)$ προκύπτει η $p(n_0+3)$. Προφανώς αυτή η διαδικασία δεν τελειώνει ποτέ. Αντιλαμβανόμαστε ότι η $p(n)$ θα είναι αληθής για κάθε ακέραιο $n \geq n_0$. Το ακόλουθο πόρισμα της πρότασης Γ΄.16 μας εξασφαλίζει ότι η μέθοδος αυτή αποτελεί μια πλήρη αποδεικτική διαδικασία.

Πόρισμα Γ΄.17. Έστω $p(n)$ ένας προτασιακός τύπος. Υποθέτουμε τα εξής:
1ο : Η πρόταση $p(n_0)$ είναι αληθής.
2ο : Ισχύει η συνεπαγωγή: $p(n)$ αληθής $\Rightarrow p(n+1)$ αληθής .
Τότε η πρόταση $p(n)$ είναι αληθής για κάθε ακέραιο $n \geq n_0$.
Απόδειξη: Έστω $\mathrm{A} = \{n \in \mathbb{Z}_{\geq n_0} \mid \text{η } p(n) \text{ είναι αληθής}\}$. Εφόσον η $p(n_0)$ είναι αληθής, έχουμε $n_0 \in \mathrm{A}$. Αν τώρα $n \in \mathrm{A}$, τότε η $p(n)$ είναι αληθής. Άρα, με βάση το 2ο βήμα, και η $p(n+1)$ είναι αληθής. Επομένως $n+1 \in \mathrm{A}$. Δηλαδή ισχύει η συνεπαγωγή $n \in \mathrm{A} \Rightarrow n+1 \in \mathrm{A}$. Με βάση την πρόταση Γ΄.16, $\mathrm{A} = \mathbb{Z}_{\geq n_0}$, δηλαδή η πρόταση είναι αληθής για κάθε ακέραιο $n \geq n_0$. ■

ΛΥΜΕΝΕΣ ΑΣΚΗΣΕΙΣ

Άσκηση 105. Να αποδείξετε ότι για κάθε θετικό ακέραιο n ισχύουν οι σχέσεις:
α) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$
β) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$
γ) $\dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \dfrac{1}{3\cdot 4} + \cdots + \dfrac{1}{n\cdot(n+1)} = \dfrac{n}{n+1}$
Απόδειξη: α) Η σχέση ισχύει για $n = 1$, γιατί και τα δύο μέλη δίνουν 1.
Υποθέτουμε λοιπόν ότι $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$ και προσθέτουμε και στα δύο μέλη το $(n+1)^2$. Έχουμε:

$$\begin{aligned}
1^2 + 2^2 + 3^2 + \cdots + n^2 + (n+1)^2 &= \left(1^2 + 2^2 + 3^2 + \cdots + n^2\right) + (n+1)^2 = \\
\text{(από την επαγωγική υπόθεση)} \quad &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \\
&= (n+1)\left(\frac{n(2n+1)}{6} + n + 1\right) = \\
&= \frac{(n+1)(2n^2 + n + 6(n+1))}{6} = \\
&= \frac{(n+1)(2n^2+7n+6)}{6} = \frac{(n+1)(2n^2+4n+3n+6)}{6} = \\
&= \frac{(n+1)(2n(n+2)+3(n+2))}{6} = \frac{(n+1)(n+2)(2n+3)}{6} = \\
&= \frac{(n+1)(n+2)(2(n+1)+1)}{6}.
\end{aligned}$$

Η απόδειξη της σχέσης **α)** ολοκληρώθηκε.
β) Η σχέση ισχύει για $n = 1$ (και τα δύο μέλη δίνουν 1). Υποθέτουμε ότι $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$. Τότε $1^3 + 2^3 + 3^3 + \cdots + n^3 + (n+1)^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3 = (n+1)^2\left(\frac{n^2}{4} + n + 1\right) = \frac{(n+1)^2(n^2+4n+4)}{4} = \frac{(n+1)^2(n+2)^2}{4}$. Η απόδειξη της σχέσης **β)** ολοκληρώθηκε.
γ) Η σχέση ισχύει για $n = 1$ (και τα δύο μέλη δίνουν $\frac{1}{2}$). Υποθέτουμε ότι $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$. Τότε θα έχουμε:
$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\cdot(n+1)} + \frac{1}{(n+1)\cdot(n+2)} = \left(\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\cdot(n+1)}\right) + \frac{1}{(n+1)\cdot(n+2)} = \frac{n}{n+1} + \frac{1}{(n+1)\cdot(n+2)} = \frac{1}{n+1}\left(n + \frac{1}{n+2}\right) = \frac{1}{n+1}\frac{n^2+2n+1}{n+2} = \frac{(n+1)^2}{(n+1)(n+2)} = \frac{n+1}{n+2} = \frac{n+1}{(n+1)+1}$. Η απόδειξη της **γ)** είναι πλήρης. ■

Άσκηση 106. (Ανισότητα Bernoulli) Αν $\varepsilon > -1$, τότε για κάθε φυσικό αριθμό n ισχύει η σχέση
$$(1+\varepsilon)^n \geq 1 + n\varepsilon.$$
Απόδειξη: Για $n = 0$ η αποδεικτέα σχέση ισχύει ως ισότητα: $(1+\varepsilon)^0 = 1 = 1 + 0\cdot\varepsilon$.
Προκειμένου να αποδείξουμε το επαγωγικό βήμα υποθέτουμε ότι $(1+\varepsilon)^n \geq 1 + n\varepsilon$, για κάποιο φυσικό αριθμό n. Επίσης, και αυτό είναι πολύ σημαντικό, παρατηρούμε ότι $1 + \varepsilon > 0$. Μπορούμε λοιπόν να πολλαπλασιάσουμε και τα δύο μέλη της σχέσης $(1+\varepsilon)^n \geq 1 + n\varepsilon$ με $1 + \varepsilon > 0$, χωρίς να αλλάξει φορά η ανισότητα.
Παίρνουμε λοιπόν: $(1+\varepsilon)^{n+1} \geq (1+\varepsilon)(1+n\varepsilon) = 1 + n\varepsilon + \varepsilon + n\varepsilon^2 = 1 + (n+1)\varepsilon + n\varepsilon^2 \underset{\varepsilon^2 \geq 0}{\geq} 1 + (n+1)\varepsilon$. ■

Παρατήρηση: Αν $\varepsilon \neq 0$, τότε στην ανισότητα Bernoulli θα έχουμε $(1+\varepsilon)^n > 1 + n\varepsilon$, για κάθε $n = 2, 3, \ldots$, όπως προκύπτει από το επαγωγικό βήμα.

Ορισμός Γ΄.18. Έστω n ακέραιος με $n \geq 0$. Ορίζουμε τον αριθμό $n!$ ο οποίος καλείται ***n*-παραγοντικό** ως εξής:
$$n! = \begin{cases} 1\cdot 2\cdots n & \text{αν } n \geq 1 \\ 1 & \text{αν } n = 0 \end{cases}$$
Ο κάπως παράδοξος ορισμός $0! = 1$ θα δικαιολογηθεί στη συνέχεια. Έτσι, $1! = 1$, $2! = 2$, $3! = 2\cdot 3 = 6$ (ο παράγοντας 1 προφανώς δεν παίζει ρόλο), $4! = 2\cdot 3\cdot 4 = 24$, $5! = 2\cdot 3\cdot 4\cdot 5 = 120$ κ.ο.κ. Παρατηρούμε επίσης ότι αν $0 \leq k < n$ τότε $n! = k!(k+1)(k+2)\cdots n$. Π.χ. $7! = 4!\cdot 5\cdot 6\cdot 7$.

Άσκηση 107. Δείξτε ότι για κάθε θετικό ακέραιο $n \geq 4$ ισχύει $n! > n^2$.
Απόδειξη: Για $n = 4$ έχουμε $4! = 24 > 16 = 4^2$. Άρα η πρόταση ισχύει για $n = 4$.
Υποθέτουμε τώρα ότι $n! > n^2$, για κάποιον ακέραιο $n \geq 4$. Τότε $(n+1)! = (n+1)n! > (n+1)n^2$. Αλλά $(n+1)n^2 > (n+1)^2 \Leftrightarrow n^2 > n+1 \Leftrightarrow n(n-1) > 1$, η οποία ισχύει γιατί $n(n-1) \geq 4\cdot 3 = 24 > 1$. Επομένως $(n+1)! > (n+1)^2$ και τελειώσαμε. ■

Άσκηση 108. α) Δείξτε ότι $\sqrt{n^n} < n!$, για κάθε $n \geq 3$.
β) Δείξτε ότι $n! < \left(\frac{n+1}{2}\right)^n$, για κάθε $n \geq 2$.

Απόδειξη: α) Για $n = 3$ έχουμε: $\sqrt{3^3} = 3\sqrt{3}$ και $3! = 6$. Αλλά $3\sqrt{3} < 6 \Leftrightarrow \sqrt{3} < 2 \Leftrightarrow 3 < 4$, δηλαδή η πρόταση είναι αληθής για $n = 3$. Υποθέτουμε ότι $n! > \sqrt{n^n}$, για κάποιο $n \geq 3$. Θα αποδείξουμε ότι $(n+1)! > \sqrt{(n+1)^{n+1}} \Leftrightarrow ((n+1)!)^2 > (n+1)^{n+1}$. Από τη σχέση $n! > \sqrt{n^n}$ παίρνουμε $(n!)^2 > n^n$. Επομένως $((n+1)!)^2 = (n+1)^2(n!)^2 > (n+1)^2 n^n$. Αρκεί να αποδείξουμε ότι $(n+1)^2 n^n \geq (n+1)^{n+1} \Leftrightarrow$ $\Leftrightarrow (n+1)n^n \geq (n+1)^n \Leftrightarrow \left(\frac{n}{n+1}\right)^n \geq \frac{1}{n+1} \Leftrightarrow \left(1 - \frac{1}{n+1}\right)^n \geq \frac{1}{n+1}$. Πράγματι, από την ανισότητα

Bernoulli, αφού $-\frac{1}{n+1} > -1$, παίρνουμε $\left(1-\frac{1}{n+1}\right)^n \geq 1-\frac{n}{n+1} = \frac{1}{n+1}$.

β) Για $n=2$ έχουμε $\left(\frac{3}{2}\right)^2 > 2 \Leftrightarrow 9 > 4\cdot 2 = 8$, η οποία είναι αληθής. Υποθέτουμε ότι $\left(\frac{n+1}{2}\right)^n > n!$, για κάποιον ακέραιο $n \geq 2$. Τότε $\left(\frac{n+2}{2}\right)^{n+1} = \frac{n+2}{2}\cdot\left(\frac{n+2}{n+1}\right)^n \cdot \left(\frac{n+1}{2}\right)^n \underset{\substack{\text{επαγωγική}\\ \text{υπόθεση}}}{>} \frac{n+2}{2}\cdot\left(\frac{n+2}{n+1}\right)^n \cdot n! =$ $= \frac{n+2}{2}\cdot\left(1+\frac{1}{n+1}\right)^n \cdot n! \underset{\substack{\text{ανισότητα}\\ \text{Bernoulli}}}{>} \frac{n+2}{2}\cdot\left(1+\frac{n}{n+1}\right)\cdot n! = \frac{(n+2)(2n+1)}{2(n+1)}\cdot n!$. Αρκεί να αποδείξουμε ότι $\frac{(n+2)(2n+1)}{2(n+1)} \geq n+1$. Η ανισότητα αυτή είναι γνήσια, όπως θα διαπιστώσουμε: $\frac{(n+2)(2n+1)}{2(n+1)} >$ $> n+1 \Leftrightarrow (n+2)(2n+1) > 2(n+1)^2 \Leftrightarrow 2n^2+5n+2 > 2n^2+4n+2 \Leftrightarrow n > 0$. ■

Άσκηση 109. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύει: $\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots+\frac{n}{2^n} = 2-\frac{n+2}{2^n}$.

Απόδειξη: Για $n=1$ το πρώτο μέλος ισούται με $\frac{1}{2}$ και το δεύτερο με $2-\frac{1+2}{2^1} = 2-\frac{3}{2} = \frac{1}{2}$. Άρα η πρόταση είναι αληθής για $n=1$.

Υποθέτουμε ότι $\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots+\frac{n}{2^n} = 2-\frac{n+2}{2^n}$.

Τότε: $\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots+\frac{n}{2^n}+\frac{n+1}{2^{n+1}} = 2-\frac{n+2}{2^n}+\frac{n+1}{2^{n+1}} = 2-\frac{2n+4}{2^{n+1}}+\frac{n+1}{2^{n+1}} = 2-\frac{2n+4-n-1}{2^{n+1}} =$ $= 2-\frac{n+3}{2^{n+1}} = 2-\frac{(n+1)+2}{2^{n+1}}$, αποδείχθηκε. ■

Άσκηση 110. Δείξτε ότι για κάθε θετικό ακέραιο n ο αριθμός $3\cdot 5^{2n-1}+2^{3n-2}$ είναι ακέραιο πολλαπλάσιο του 17.

Απόδειξη: Για $n=1$ έχουμε: $3\cdot 5^{2n-1}+2^{3n-2} = 3\cdot 5+2 = 15+2 = 17 = 1\cdot 17$.

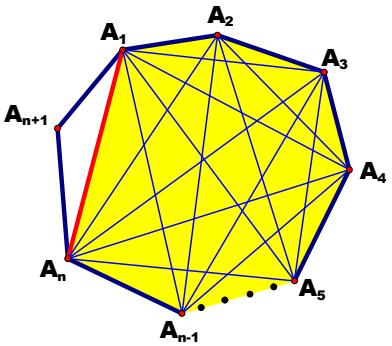
Υποθέτουμε ότι για κάποιο θετικό ακέραιο n ο αριθμός $3\cdot 5^{2n-1}+2^{3n-2}$ είναι πολλαπλάσιο του 17, δηλαδή $3\cdot 5^{2n-1}+2^{3n-2} = 17\lambda$, όπου $\lambda \in \mathbb{Z}$.

Τότε για $n+1$ θα έχουμε: $3\cdot 5^{2(n+1)-1}+2^{3(n+1)-2} = 3\cdot 5^{2n-1}\cdot 5^2+2^{3n-2}\cdot 2^3 = 3\cdot 5^{2n-1}\cdot 25+2^{3n-2}\cdot 8 =$ $= 3\cdot 5^{2n-1}\cdot(17+8)+2^{3n-2}\cdot 8 = 3\cdot 5^{2n-1}\cdot 17+3\cdot 5^{2n-1}\cdot 8+2^{3n-2}\cdot 8 = 3\cdot 5^{2n-1}\cdot 17+8\cdot(3\cdot 5^{2n-1}+2^{3n-2}) =$ $= 17\cdot 3\cdot 5^{2n-1}+17\cdot 8\lambda = 17(3\cdot 5^{2n-1}+8\lambda)$. Προφανώς ο αριθμός $3\cdot 5^{2n-1}+8\lambda$ είναι ακέραιος και κατά συνέπεια $3\cdot 5^{2(n+1)-1}+2^{3(n+1)-2}$ είναι ακέραιο πολλαπλάσιο του 17. ■

Άσκηση 111. Κάθε κυρτό πολύγωνο με n κορυφές έχει $\frac{n(n-3)}{2}$ διαγωνίους.

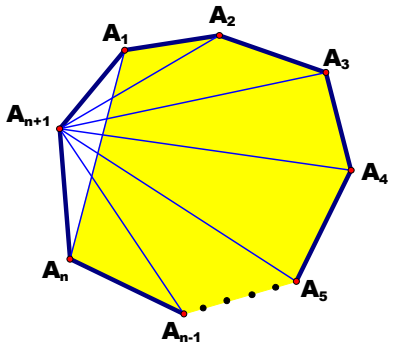
Απόδειξη: Κατ' αρχάς σημειώνουμε ότι $n \geq 3$. Για $n=3$ το τρίγωνο δεν έχει διαγωνίους ή ισοδύναμα έχει 0 διαγωνίους. Όμως $\frac{3(3-3)}{2} = 0$ και άρα ο τύπος $\frac{n(n-3)}{2}$ δουλεύει για $n=3$. Υποθέτουμε τώρα ότι κάθε κυρτό πολύγωνο με n κορυφές έχει $\frac{n(n-3)}{2}$ διαγωνίους, όπου το $n \geq 3$ είναι ακέραιος.

Με αυτό ως δεδομένο, θεωρούμε ένα κυρτό πολύγωνο $A_1A_2A_3\ldots A_nA_{n+1}$ με $n+1$ κορυφές.



Σχήμα 11

Ενώνουμε την κορυφή A_n με την κορυφή A_1, οπότε παίρνουμε το πολύγωνο $A_1A_2A_3\dots A_n$. Προφανώς κάθε διαγώνιος του $A_1A_2A_3\dots A_n$ είναι και διαγώνιος του $A_1A_2A_3\dots A_nA_{n+1}$. Από την επαγωγική υπόθεση προκύπτει ότι το πλήθος των διαγωνίων του $A_1A_2A_3\dots A_n$ ισούται με $\dfrac{n(n-3)}{2}$.
Απομένουν οι διαγώνιοι του $A_1A_2A_3\dots A_nA_{n+1}$ που δεν είναι διαγώνιοι του $A_1A_2A_3\dots A_n$. Ποιες και πόσες το πλήθος είναι αυτές;



Σχήμα 12

Όπως φαίνεται στο σχήμα αυτές είναι όλες οι διαγώνιοι που ξεκινούν από το A_{n+1} συν τη διαγώνιο A_nA_1, η οποία είναι πλευρά του $A_1A_2A_3\dots A_n$ και δεν μετρήθηκε προηγουμένως. Οι διαγώνιοι που ξεκινούν από το A_{n+1} είναι όσες και τα σημεία $A_2, A_3, A_4, \dots, A_{n-1}$. (Τα σημεία A_1 και A_n εξαιρούνται). Επομένως έχουμε $(n-1)-2+1=n-2$ διαγωνίους συν την διαγώνιο A_nA_1. Σύνολο $n-1$ επιπλέον διαγώνιοι. Κατά συνέπεια ο συνολικός αριθμός των διαγωνίων του $A_1A_2A_3\dots A_nA_{n+1}$ ισούται με:
$\dfrac{n(n-3)}{2}+n-1=\dfrac{n^2-3n}{2}+n-1=\dfrac{n^2-3n+2n-2}{2}=\dfrac{n^2+2n+1-3n-3}{2}=\dfrac{(n+1)^2-3(n+1)}{2}=$
$=\dfrac{(n+1)((n+1)-3)}{2}$, δηλαδή προκύπτει ο ίδιος τύπος με $n+1$ στη θέση του n. ■

Άσκηση 112. Να αποδείξετε ότι για κάθε θετικό ακέραιο n ισχύει ταυτότητα:
$$\alpha^n-\beta^n=(\alpha-\beta)(\alpha^{n-1}+\alpha^{n-2}\beta+\alpha^{n-3}\beta^2+\dots+\alpha^2\beta^{n-3}+\alpha\beta^{n-2}+\beta^{n-1})$$
Απόδειξη: Για $n=1$ έχουμε $\alpha^1-\beta^1=(\alpha-\beta)\alpha^0\beta^0$ (το άθροισμα της παρένθεσης ισούται με $\alpha^0\beta^0$) και άρα ο τύπος ισχύει σ' αυτή την περίπτωση.
Υποθέτουμε ότι $\alpha^n-\beta^n=(\alpha-\beta)(\alpha^{n-1}+\alpha^{n-2}\beta+\dots+\alpha\beta^{n-2}+\beta^{n-1})$. Τότε έχουμε:
$$\alpha^{n+1}-\beta^{n+1}=\alpha^{n+1}-\alpha^n\beta+\alpha^n\beta-\beta^{n+1}=\alpha^n(\alpha-\beta)+\beta(\alpha^n-\beta^n).$$
Αλλά $\alpha^n-\beta^n=(\alpha-\beta)(\alpha^{n-1}+\alpha^{n-2}\beta+\dots+\alpha\beta^{n-2}+\beta^{n-1})$, λόγω της επαγωγικής υπόθεσης.
Επομένως
$$\begin{aligned}\alpha^{n+1}-\beta^{n+1}&=\alpha^n(\alpha-\beta)+\beta(\alpha-\beta)(\alpha^{n-1}+\alpha^{n-2}\beta+\dots+\alpha\beta^{n-2}+\beta^{n-1})=\\&=(\alpha-\beta)\left(\alpha^n+\beta(\alpha^{n-1}+\alpha^{n-2}\beta+\dots+\alpha\beta^{n-2}+\beta^{n-1}\right)=\\&=(\alpha-\beta)(\alpha^n+\alpha^{n-1}\beta+\alpha^{n-2}\beta^2+\dots+\alpha\beta^{n-1}+\beta^n)\end{aligned}$$
και άρα ο τύπος ισχύει και για $n+1$. ■

Άσκηση 113. Δείξτε ότι για κάθε ακέραιο $n\geq 2$ ισχύει: $1+\dfrac{1}{\sqrt{2}}+\dfrac{1}{\sqrt{3}}+\dots+\dfrac{1}{\sqrt{n}}>\sqrt{n}$.

Απόδειξη: Για $n=2$ έχουμε: $1+\dfrac{1}{\sqrt{2}}>\sqrt{2}\Leftrightarrow\sqrt{2}+1>2\Leftrightarrow\sqrt{2}>1$, που ισχύει.

Υποθέτουμε ότι, για κάποιο n ισχύει ότι $1+\dfrac{1}{\sqrt{2}}+\dfrac{1}{\sqrt{3}}+\dots+\dfrac{1}{\sqrt{n}}>\sqrt{n}$.

Θα αποδείξουμε ότι $1+\dfrac{1}{\sqrt{2}}+\dfrac{1}{\sqrt{3}}+\dots+\dfrac{1}{\sqrt{n}}+\dfrac{1}{\sqrt{n+1}}>\sqrt{n+1}$.

Πράγματι, $1+\dfrac{1}{\sqrt{2}}+\dfrac{1}{\sqrt{3}}+\dots+\dfrac{1}{\sqrt{n}}+\dfrac{1}{\sqrt{n+1}}=\left(1+\dfrac{1}{\sqrt{2}}+\dfrac{1}{\sqrt{3}}+\dots+\dfrac{1}{\sqrt{n}}\right)+\dfrac{1}{\sqrt{n+1}}>\sqrt{n}+\dfrac{1}{\sqrt{n+1}}$,
λόγω της επαγωγικής υπόθεσης.

Αρκεί να δείξουμε ότι $\sqrt{n}+\dfrac{1}{\sqrt{n+1}} \geq \sqrt{n+1}$. Θα δείξουμε την «ισχυρότερη» ανισότητα $\sqrt{n}+\dfrac{1}{\sqrt{n+1}} > > \sqrt{n+1}$. Πράγματι, $\sqrt{n}+\dfrac{1}{\sqrt{n+1}} > \sqrt{n+1} \Leftrightarrow \sqrt{n(n+1)}+1 > n+1 \Leftrightarrow \sqrt{n(n+1)} > n \Leftrightarrow n^2+n > > n^2 \Leftrightarrow n > 0$. ■

Άσκηση 114. Δείξτε ότι για κάθε ακέραιο $n \geq 3$ ισχύει: $n^{n+1} > (n+1)^n$.
Απόδειξη: Για $n=3$ η αποδεικτέα σχέση γίνεται $3^4 > 4^3 \Leftrightarrow 81 > 64$, η οποία είναι προφανώς αληθής.
Υποθέτουμε ότι, για κάποιο n ισχύει $n^{n+1} > (n+1)^n$. Θα δείξουμε ότι $(n+1)^{n+2} > (n+2)^{n+1}$.
Έχουμε: $(n+1)^{n+2} = \dfrac{(n+1)^{n+2}}{n^{n+1}} n^{n+1} \underset{\substack{\text{επαγωγική}\\ \text{υπόθεση}}}{>} \dfrac{(n+1)^{n+2}}{n^{n+1}}(n+1)^n = \dfrac{(n+1)^{2n+2}}{n^{n+1}} = \left(\dfrac{(n+1)^2}{n}\right)^{n+1}$.
Αρκεί να δείξουμε ότι $\left(\dfrac{(n+1)^2}{n}\right)^{n+1} > (n+2)^{n+1} \Leftrightarrow \dfrac{(n+1)^2}{n} > n+2 \Leftrightarrow n^2+2n+1 > n^2+2n \Leftrightarrow 1>0$, η οποία ισχύει. ■

Άσκηση 115. (Ανισότητα Cauchy) Αν $\alpha_1, \alpha_2, \ldots, \alpha_n$ και $\beta_1, \beta_2, \ldots, \beta_n$ είναι πραγματικοί αριθμοί, τότε ισχύει η ανισότητα

$$(\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2)\,(\beta_1^2+\beta_2^2+\cdots+\beta_n^2) \geq (\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n)^2$$

Απόδειξη: Για $n=1$ παίρνουμε την ισότητα $\alpha_1^2\beta_1^2 = \alpha_1^2\beta_1^2$.
Υποθέτουμε ότι $(\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2)\,(\beta_1^2+\beta_2^2+\cdots+\beta_n^2) \geq (\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n)^2$.
Τότε $(\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2+\alpha_{n+1}^2)(\beta_1^2+\beta_2^2+\cdots+\beta_n^2+\beta_{n+1}^2) = (\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2)(\beta_1^2+\beta_2^2+\cdots+\beta_n^2)+(\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2)\beta_{n+1}^2+\alpha_{n+1}^2(\beta_1^2+\beta_2^2+\cdots+\beta_n^2)+\alpha_{n+1}^2\beta_{n+1}^2 \geq \underbrace{(\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n)^2}_{\text{επαγωγική υπόθεση}}+(\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2)\beta_{n+1}^2+$
$+\alpha_{n+1}^2(\beta_1^2+\beta_2^2+\cdots+\beta_n^2)+\alpha_{n+1}^2\beta_{n+1}^2 =$
$= \underbrace{\left((\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n)^2+\alpha_{n+1}^2\beta_{n+1}^2+2(\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n)\alpha_{n+1}\beta_{n+1}\right)}_{\text{τέλειο τετράγωνο}} -$
$-2(\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n)\alpha_{n+1}\beta_{n+1}+(\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2)\beta_{n+1}^2+\alpha_{n+1}^2(\beta_1^2+\beta_2^2+\cdots+\beta_n^2) = (\alpha_1\beta_1+\alpha_2\beta_2+\cdots+$
$+\alpha_n\beta_n+\alpha_{n+1}\beta_{n+1})^2+(\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2)\beta_{n+1}^2+\alpha_{n+1}^2(\beta_1^2+\beta_2^2+\cdots+\beta_n^2)-2(\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n)\alpha_{n+1}\beta_{n+1} =$
$= (\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n+\alpha_{n+1}\beta_{n+1})^2+$

$$\textbf{(τέλεια τετράγωνα)}\begin{cases}+(\alpha_1^2\beta_{n+1}^2+\alpha_{n+1}^2\beta_1^2-2\alpha_1\beta_1\alpha_{n+1}\beta_{n+1})+\\ +(\alpha_2^2\beta_{n+1}^2+\alpha_{n+1}^2\beta_2^2-2\alpha_2\beta_2\alpha_{n+1}\beta_{n+1})+\\ +(\alpha_3^2\beta_{n+1}^2+\alpha_{n+1}^2\beta_3^2-2\alpha_3\beta_3\alpha_{n+1}\beta_{n+1})+\cdots+\\ +(\alpha_n^2\beta_{n+1}^2+\alpha_{n+1}^2\beta_n^2-2\alpha_n\beta_n\alpha_{n+1}\beta_{n+1}) =\end{cases}$$

$= (\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n+\alpha_{n+1}\beta_{n+1})^2+(\alpha_1\beta_{n+1}-\alpha_{n+1}\beta_1)^2+(\alpha_2\beta_{n+1}-\alpha_{n+1}\beta_2)^2+\cdots+(\alpha_n\beta_{n+1}+$
$+\alpha_{n+1}\beta_n)^2 \geq (\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n+\alpha_{n+1}\beta_{n+1})^2$. ■

Άσκηση 116. Αν ένα σύνολο Α έχει n στοιχεία, όπου $n \in \mathbb{N}$, τότε $|\mathcal{P}(\mathrm{A})| = 2^n$.
Απόδειξη: Για $n=0$, δηλαδή $\mathrm{A}=\varnothing$, το μοναδικό υποσύνολο του Α είναι το κενό. Επομένως $\mathcal{P}(\mathrm{A})=\{\varnothing\}$ και κατά συνέπεια $|\mathcal{P}(\mathrm{A})| = 1 = 2^0$. Αν $\mathrm{A}=\{\alpha\}$, μονοσύνολο, τότε $\mathcal{P}(\mathrm{A})=\{\varnothing,\{\alpha\}\}$. Επομένως $|(\mathrm{A})| = 2 = 2^1$.
Υποθέτουμε ότι η πρόταση είναι αληθής για κάποιο $n \geq 0$. Θα αποδείξουμε ότι ισχύει και για $n+1$.
Έστω Α$=\{\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}\}$ ένα σύνολο με $n+1$ στοιχεία. Χωρίζουμε τα υποσύνολα του Α σε δύο ομάδες: Την ομάδα $\mathcal{D}$, η οποία αποτελείται από τα υποσύνολα του Α **που περιέχουν το** α_1 και την ομάδα $\mathcal{D}'$, η οποία αποτελείται από τα υποσύνολα του Α **που δεν περιέχουν το** α_1.
Τα υποσύνολα του Α που δεν περιέχουν το α_1 είναι ακριβώς όλα τα υποσύνολα του $\mathrm{A}'=\{\alpha_2, \ldots, \alpha_n, \alpha_{n+1}\}$, το οποίο περιέχει ακριβώς n στοιχεία. Δηλαδή $\mathcal{D}'=\mathcal{P}(\mathrm{A}')$. Λόγω της επαγωγικής υπόθεσης αυτά είναι 2^n το πλήθος, δηλαδή $|\mathcal{D}'|=2^n$.
Τώρα, από κάθε υποσύνολο του Α που περιέχει το α_1 αφαιρούμε το στοιχείο α_1 και παίρνουμε έτσι ένα μοναδικό υποσύνολο του Α′. Ορίζεται λοιπόν μια απεικόνιση $f : \mathcal{D} \to \mathcal{D}' = \mathcal{P}(\mathrm{A}')$, με τύπο $f(\mathrm{X}) = \mathrm{X} \setminus \{\alpha_1\}$, για κάθε $\mathrm{X} \in \mathcal{D}$. Επειδή κάθε σύνολο $\mathrm{X} \in \mathcal{D}$ γράφεται κατά τρόπο μοναδικό στη

μορφή $\mathrm{X} = \mathrm{X}' \cup \{\alpha_1\}$, όπου $\mathrm{X}' \in \mathcal{D}' = \mathcal{P}(\mathrm{A}')$, η f είναι μια αμφιμονοσήμαντη αντιστοιχία (1-1 και επί) ανάμεσα στις $\mathcal{D}$ και $\mathcal{D}'$. Έτσι, $|\mathcal{D}| = |\mathcal{D}'| = 2^n$. Επειδή προφανώς $\mathcal{D} \cap \mathcal{D}' = \varnothing$ και $\mathcal{P}(\mathrm{A}) = \mathcal{D} \cup \mathcal{D}'$, έπεται ότι $|\mathcal{P}(\mathrm{A})| = |\mathcal{D}| + |\mathcal{D}'| = 2^n + 2^n = 2^{n+1}$. ■

Παρατήρηση: Λόγω της σχέσης $|\mathcal{P}(A)| = 2^{|A|}$ η οποία συνδέει τον πληθάριθμο ενός συνόλου A με αυτόν του δυναμοσυνόλου του, πολλές φορές στη βιβλιογραφία το δυναμοσύνολο $\mathcal{P}(A)$ του A συμβολίζεται με 2^A, ακόμη και στην περίπτωση που το A έχει άπειρα στοιχεία.

Από τα προηγούμενα παραδείγματα καθίσταται φανερό ότι η απόδειξη του επαγωγικού βήματος είναι συνήθως το πιο δύσκολο σημείο σε μια επαγωγική απόδειξη[1]. Η αντίληψη αυτή πολλές φορές μας οδηγεί στην εσφαλμένη εντύπωση ότι η επαλήθευση μιας πρότασης για την (ή τις) αρχική(-κές) τιμή(-ές) του n είναι ίσως περιττή. Τούτη όμως η αντίληψη ελοχεύει κινδύνους. Πράγματι, ας παρατηρήσουμε την παρακάτω «απόδειξη»:
Ας υποθέσουμε ότι μας ζητείται να αποδείξουμε ότι $n = n + 2$. (!) Είναι προφανές ότι η σχέση αυτή δεν είναι δυνατόν να ισχύει.
Και όμως· αν υποθέσουμε ότι η σχέση αυτή ισχύει για κάποιο n, δηλαδή $n = n + 2$, τότε προσθέτοντας και στα δύο μέλη το 1, προκύπτει ότι $n + 1 = (n + 1) + 2$, δηλαδή η πρόταση ισχύει και για $n + 1$.
Είναι όμως προφανές ότι η σχέση $n = n + 2$ είναι αδύνατη. Πού βρίσκεται το λάθος; Μα φυσικά στην έλλειψη του $1^{\text{ου}}$ βήματος. Θα έπρεπε να αποδείξουμε ότι $1 = 1 + 2 = 3$, πράγμα αδύνατον.
Και για να χρησιμοποιήσουμε το σχήμα του ντόμινο στην περίπτωσή μας: Δεν αρκεί να τοποθετήσουμε τα στρατιωτάκια κατά τέτοιον τρόπο ώστε αν πέσει κάποιο, τότε θα πέσει και το επόμενό του. Θα πρέπει να ρίξουμε το πρώτο στρατιωτάκι αλλιώς δεν πέφτει κανένα!

Άσκηση 117. (Ορίζουσα Vandermonde) Έστω $x_1, x_2, \ldots, x_n$ μεταβλητές. Η ορίζουσα

$$D(x_1, x_2, \ldots, x_n) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$$

ονομάζεται **ορίζουσα του Vandermonde**[2]. Δείξτε ότι $D(x_1, x_2, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i)$.

Απόδειξη: Για $n = 2$ έχουμε $D(x_1, x_2) = \begin{vmatrix} 1 & 1 \\ x_1 & x_2 \end{vmatrix} = x_2 - x_1$. Ο τύπος ισχύει λοιπόν για $n = 2$. Τώρα, η ορίζουσα $D(x_1, x_2, \ldots, x_n)$ γράφεται πιο αναλυτικά ως εξής: $D(x_1, x_2, \ldots, x_n) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-3} & x_2^{n-3} & \cdots & x_n^{n-3} \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$.
Αν αφαιρέσουμε από την τελευταία γραμμή την προτελευταία, πολλαπλασιασμένη επί x_1, θα πάρουμε

$$D(x_1, x_2, \ldots, x_n) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-3} & x_2^{n-3} & \cdots & x_n^{n-3} \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\ 0 & x_2^{n-1} - x_1 x_2^{n-2} & \cdots & x_n^{n-1} - x_1 x_n^{n-2} \end{vmatrix} =$$

[1] Αυτό δεν είναι πάντοτε ο κανόνας.

[2] Όπως αναφέρεται από τους ιστορικούς των Μαθηματικών, ο Vandermonde δεν χρησιμοποίησε ποτέ τη συγκεκριμένη ορίζουσα. Κακώς λοιπόν φέρει το όνομά του.

$$= \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-3} & x_2^{n-3} & \cdots & x_n^{n-3} \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\ 0 & (x_2-x_1)x_2^{n-2} & \cdots & (x_n-x_1)x_n^{n-2} \end{vmatrix}.$$

Αν αφαιρέσουμε από την $(n-1)$-στη γραμμή την $(n-2)$-στη γραμμή, πολλαπλασιασμένη επί x_1, θα πάρουμε την ορίζουσα

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-3} & x_2^{n-3} & \cdots & x_n^{n-3} \\ 0 & x_2^{n-2}-x_1x_2^{n-3} & \cdots & x_n^{n-2}-x_1x_n^{n-3} \\ 0 & (x_2-x_1)x_2^{n-2} & \cdots & (x_n-x_1)x_n^{n-2} \end{vmatrix} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-3} & x_2^{n-3} & \cdots & x_n^{n-3} \\ 0 & (x_2-x_1)x_2^{n-3} & \cdots & (x_n-x_1)x_n^{n-3} \\ 0 & (x_2-x_1)x_2^{n-2} & \cdots & (x_n-x_1)x_n^{n-2} \end{vmatrix}.$$

Προχωρώντας κατ᾽ αυτόν τον τρόπο, μέχρι να αφαιρέσουμε από τη δεύτερη γραμμή την πρώτη, πολλαπλασιασμένη επί x_1, θα καταλήξουμε στη μορφή

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & x_2-x_1 & x_3-x_1 & \cdots & x_n-x_1 \\ 0 & (x_2-x_1)x_2 & (x_3-x_1)x_3 & \cdots & (x_n-x_1)x_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & (x_2-x_1)x_2^{n-3} & (x_3-x_1)x_3^{n-3} & \cdots & (x_n-x_1)x_n^{n-3} \\ 0 & (x_2-x_1)x_2^{n-2} & (x_3-x_1)x_3^{n-2} & \cdots & (x_n-x_1)x_n^{n-2} \end{vmatrix} =$$

$$= \begin{vmatrix} x_2-x_1 & x_3-x_1 & \cdots & x_n-x_1 \\ (x_2-x_1)x_2 & (x_3-x_1)x_3 & \cdots & (x_n-x_1)x_n \\ \vdots & \vdots & \ddots & \vdots \\ (x_2-x_1)x_2^{n-3} & (x_3-x_1)x_3^{n-3} & \cdots & (x_n-x_1)x_n^{n-3} \\ (x_2-x_1)x_2^{n-2} & (x_3-x_1)x_3^{n-2} & \cdots & (x_n-x_1)x_n^{n-2} \end{vmatrix} =$$

$$= (x_2-x_1)(x_3-x_1)\cdots(x_n-x_1)\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_2 & x_3 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_2^{n-3} & x_3^{n-3} & \cdots & x_n^{n-3} \\ x_2^{n-2} & x_3^{n-2} & \cdots & x_n^{n-2} \end{vmatrix} = (x_2-x_1)(x_3-x_1)\cdots(x_n-x_1)D(x_2,\ldots,x_n).$$

Αν λοιπόν υποθέσουμε ότι ο τύπος ισχύει για $n-1$ μεταβλητές, τότε $D(x_2,\ldots,x_n) = \prod_{2\le i<j\le n}(x_j-x_i)$.

Επομένως $D(x_1,x_2,\ldots,x_n) = (x_2-x_1)(x_3-x_1)\cdots(x_n-x_1)\prod_{2\le i<j\le n}(x_j-x_i) = \prod_{1\le i<j\le n}(x_j-x_i)$. ■

Σημείωση: Εδώ το επαγωγικό βήμα ήταν από $n-1$ σε n. Αυτό βέβαια δεν αλλάζει τίποτα. Είναι θέμα συμβολισμού.

ΑΛΥΤΕΣ ΑΣΚΗΣΕΙΣ

78. Να αποδείξετε ότι $1+3+5+7+\cdots+(2n-1)=n^2$.

79. Να αποδείξετε ότι $\frac{1}{1\cdot2\cdot3}+\frac{1}{2\cdot3\cdot4}+\frac{1}{3\cdot4\cdot5}+\cdots+\frac{1}{n(n+1)(n+2)} = \frac{1}{4}-\frac{1}{2(n+1)(n+2)}$.

80. Να αποδείξετε ότι $\frac{1}{2\cdot3\cdot4}+\frac{2}{3\cdot4\cdot5}+\frac{3}{4\cdot5\cdot6}+\cdots+\frac{n}{(n+1)(n+2)(n+3)} = \frac{n(n+1)}{4(n+2)(n+3)}$.

81. Δείξτε ότι $1\cdot2^1+2\cdot2^2+3\cdot2^3+\cdots+n\cdot2^n=(n-1)2^{n+1}+2$.

82. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύει η σχέση: $1-2^2+3^2-4^2+\cdots+(-1)^{n-1}n^2=(-1)^{n-1}\cdot\frac{n(n+1)}{2}$.

83. Δείξτε ότι αν α είναι θετικός πραγματικός αριθμός και n θετικός ακέραιος, τότε ισχύει:
$\frac{1}{\alpha(\alpha+1)} + \frac{1}{(\alpha+1)(\alpha+2)} + \cdots + \frac{1}{(\alpha+n-1)(\alpha+n)} = \frac{n}{\alpha(\alpha+n)}$.

84. Αν $x \neq \pm 1$ και n μη αρνητικός ακέραιος, τότε ισχύει:
$\frac{1}{1+x} + \frac{2}{1+x^2} + \frac{4}{1+x^4} + \frac{8}{1+x^8} + \cdots + \frac{2^n}{1+x^{2^n}} = \frac{1}{x-1} + \frac{2^{n+1}}{1-x^{2^{n+1}}}$. .

85. Δείξτε ότι αν $x \neq 1$, τότε για κάθε θετικό ακέραιο n ισχύει η σχέση: $1 + 2x + 3x^2 + \cdots + nx^{n-1} = \frac{1-x^n}{(1-x)^2} - \frac{nx^n}{1-x}$.

86. Να δείξετε ότι για κάθε $n \geq 2$ ισχύει: $\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{16}\right) \cdots \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}$.

87. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύει η σχέση: $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1$.

88. Να αποδείξετε ότι για κάθε $n \geq 6$ ισχύει: $n! > n^3$.

89. Αν $\alpha, \beta > 0$ με $\alpha + \beta = 1$, να δείξετε ότι για κάθε θετικό ακέραιο n ισχύει: $\alpha^{2^n} + \beta^{2^n} \geq \frac{1}{2^{2^n-1}}$.

90. Να αποδείξετε ότι για κάθε ακέραιο n με $n \geq 3$ ισχύει: $4^n + 5^n < 6^n$.

91. Δείξτε ότι για κάθε $n \geq 4$ ισχύουν οι σχέσεις: $3^{n-1} > n^2$ και $\sqrt[3]{3} > \sqrt[n]{n}$.

92. Δείξτε ότι αν $n > 1$, τότε $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < \frac{2n}{n+1}$.

93. Δείξτε ότι για κάθε θετικό ακέραιο $n \geq 3$ ισχύει: $\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \leq \frac{7}{10} - \frac{1}{2(n+1)}$.

94. Να αποδείξετε ότι για κάθε θετικό ακέραιο n ο αριθμός $5^n + 8^{3n-2}$ είναι πολλαπλάσιο του 13.

95. Να αποδείξετε ότι για κάθε ακέραιο $n \geq 0$ ο αριθμός $11^{n+2} + 12^{2n+1}$ είναι πολλαπλάσιο του 133.

96. Αν x είναι θετικός πραγματικός αριθμός και n ακέραιος με $n \geq 2$, τότε $(1+x)^n \geq 1 + nx + \frac{n(n-1)}{2}x^2$.

97. Να δείξετε ότι αν $\varepsilon > -1$ και $n > 1$, τότε ισχύει η ισοδυναμία: $(1+\varepsilon)^n = 1 + n\varepsilon \Leftrightarrow \varepsilon = 0$. (*Υπόδειξη: Δείτε ξανά το επαγωγικό βήμα στην απόδειξη της ανισότητας Bernoulli*).

98. Αν $0 < \alpha < \frac{1}{n}$, να δείξετε ότι $(1+\alpha)^n < \frac{1}{1-n\alpha}$, για κάθε $n = 1, 2, \ldots$ (*Υπόδειξη: Χρησιμοποιείστε την ανισότητα Bernoulli*).

99. Δείξτε ότι για κάθε θετικό ακέραιο $n \geq 2$ ισχύει: $2\left(\sqrt{n+1} - 1\right) < 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n} - 1$.

100. Δείξτε ότι αν $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι πραγματικοί αριθμοί μεγαλύτεροι ή ίσοι του μηδενός, τότε ισχύει η ανισότητα: $\frac{\alpha_1+\alpha_2+\cdots+\alpha_n}{1+\alpha_1+\alpha_2+\cdots+\alpha_n} \leq \frac{\alpha_1}{1+\alpha_1} + \frac{\alpha_2}{1+\alpha_2} + \cdots + \frac{\alpha_n}{1+\alpha_n}$.

101. (Ανισότητα Weierstrass ή επί το γερμανικότερον Weierstraß) Αν $\alpha_1, \alpha_2, \ldots, \alpha_n > 0$, τότε
$$(1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_n) > 1 + \alpha_1 + \alpha_2 + \cdots + \alpha_n, \text{ για κάθε } n \geq 2.$$

102. Αν $\alpha_1, \alpha_2, \ldots, \alpha_n > 0$, δείξτε ότι $(\alpha_1 + \alpha_2 + \cdots + \alpha_n)\left(\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \cdots + \frac{1}{\alpha_n}\right) \geq n^2$.

103. (Ανισότητα Chebyshev) Αν $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_n$ και $\beta_1 \leq \beta_2 \leq \ldots \leq \beta_n$, δείξτε ότι
$$(\alpha_1 + \alpha_2 + \cdots + \alpha_n)(\beta_1 + \beta_2 + \cdots + \beta_n) \leq n \cdot (\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_n\beta_n).$$

104. Δείξτε ότι αν $\alpha, \beta > 0$ και $n = 1, 2, \ldots$, τότε $\frac{\alpha^n+\beta^n}{2} \geq \left(\frac{\alpha+\beta}{2}\right)^n$. (*Υπόδειξη: Μπορούμε να υποθέσουμε ότι* $\alpha \leq \beta$. *Τότε* $\frac{\alpha^{n+1}+\beta^{n+1}}{2} = \frac{\alpha^{n+1}+\alpha\beta^n-\alpha\beta^n+\beta^{n+1}}{2} = \ldots$)

Ορισμός Γ΄.19. Έστω $\alpha_1, \alpha_2, \ldots, \alpha_n$ μη αρνητικοί πραγματικοί αριθμοί. Ο αριθμός $\frac{\alpha_1 + \alpha_2 + \cdots + \alpha_n}{n}$ λέγεται **αριθμητικός μέσος** και ο αριθμός $\sqrt[n]{\alpha_1 \cdot \alpha_2 \cdots \alpha_n}$ **γεωμετρικός μέσος** των $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Άσκηση 118. (Ανισότητα Αριθμητικού-Γεωμετρικού Μέσου) Έστω $\alpha_1, \alpha_2, \ldots, \alpha_n$ μη αρνητικοί πραγματικοί αριθμοί. Τότε ο αριθμητικός μέσος είναι μεγαλύτερος ή ίσος του γεωμετρικού τους μέσου, δηλαδή

$$\frac{\alpha_1+\alpha_2+\cdots+\alpha_n}{n} \geq \sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}$$

Επιπροσθέτως η παραπάνω σχέση ισχύει ως ισότητα αν και μόνον αν $\alpha_1=\alpha_2=\cdots=\alpha_n$.
Παρακάτω θα δώσουμε τέσσερις αποδείξεις της ανισότητας αυτής.
1η Απόδειξη: Κατ' αρχάς παρατηρούμε ότι αν κάποιος από τους $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι μηδέν, τότε το δεύτερο μέλος της αποδεικτέας σχέσης μηδενίζεται. Άρα σ' αυτή την περίπτωση η σχέση ισχύει κατά τετριμμένο τρόπο. (Γιατί $\alpha_1, \alpha_2, \ldots, \alpha_n \geq 0$). Στην περίπτωση αυτή η σχέση ισχύει ως ισότητα αν και μόνον αν $\alpha_1=\alpha_2=\cdots=\alpha_n=0$. Έτσι στα επόμενα, αλλά και στις άλλες αποδείξεις που θα ακολουθήσουν υποθέτουμε ότι οι αριθμοί $\alpha_1, \alpha_2, \ldots, \alpha_n$ **είναι θετικοί**.
Αποδεικνύουμε πρώτα την ανισότητα στην περίπτωση που το n είναι δύναμη του 2. Υποθέτουμε λοιπόν ότι $n=2^k$, όπου k ένας μη αρνητικός ακέραιος. Εφαρμόζουμε επαγωγή επί του k.
Αν $k=0$, δηλαδή $n=2^0=1$, τότε έχουμε ακριβώς έναν αριθμό $\alpha_1>0$ και η σχέση που πρέπει να αποδείξουμε είναι η $\frac{\alpha_1}{1} \geq \sqrt[1]{\alpha_1}$, δηλαδή $\alpha_1 \geq \alpha_1$, η οποία ισχύει βεβαίως ως ισότητα.
Στην περίπτωση που $k=1$ και άρα $n=2$ έχουμε δύο αριθμούς α_1 και α_2 και πρέπει να αποδείξουμε ότι $\frac{\alpha_1+\alpha_2}{2} \geq \sqrt{\alpha_1\alpha_2} \Leftrightarrow \alpha_1+\alpha_2 \geq 2\sqrt{\alpha_1\alpha_2} \Leftrightarrow (\sqrt{\alpha_1}-\sqrt{\alpha_2})^2 \geq 0$, η οποία είναι αληθής. Ισχύει δε ως ισότητα αν και μόνον αν $\sqrt{\alpha_1}=\sqrt{\alpha_2} \Leftrightarrow \alpha_1=\alpha_2$.
Υποθέτουμε ότι η ανισότητα είναι αληθής για κάθε 2^k μη αρνητικούς αριθμούς $\alpha_1, \alpha_2, \ldots, \alpha_{2^k}$, δηλαδή

$$\frac{\alpha_1+\alpha_2+\cdots+\alpha_{2^k}}{2^k} \geq \sqrt[2^k]{\alpha_1\alpha_2\cdots\alpha_{2^k}}. \quad \textbf{(1)}$$

και ότι ισχύει ως ισότητα αν και μόνον αν $\alpha_1=\alpha_2=\cdots=\alpha_{2^k}$.
Θεωρούμε τώρα 2^{k+1} μη αρνητικούς αριθμούς $\alpha_1, \alpha_2, \ldots, \alpha_{2^k}, \alpha_{2^k+1}, \alpha_{2^k+2}, \ldots, \alpha_{2^{k+1}}$. Παρατηρούμε ότι

$$\frac{\alpha_1+\alpha_2+\cdots+\alpha_{2^k}+\alpha_{2^k+1}+\alpha_{2^k+2}+\cdots+\alpha_{2^{k+1}}}{2^{k+1}} = \frac{\frac{\alpha_1+\cdots+\alpha_{2^k}}{2^k}+\frac{\alpha_{2^k+1}+\cdots+\alpha_{2^{k+1}}}{2^k}}{2}. \quad \textbf{(2)}$$

Λόγω της επαγωγικής υπόθεσης οι αριθμοί $\frac{\alpha_1+\alpha_2+\cdots+\alpha_{2^k}}{2^k}$ και $\frac{\alpha_{2^k+1}+\alpha_{2^k+2}+\cdots+\alpha_{2^{k+1}}}{2^k}$ είναι μεγαλύτεροι ή ίσοι των $\sqrt[2^k]{\alpha_1\alpha_2\cdots\alpha_{2^k}}$ και $\sqrt[2^k]{\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}}$ αντίστοιχα. Επομένως

$$\frac{\frac{\alpha_1+\alpha_2+\cdots+\alpha_{2^k}}{2^k}+\frac{\alpha_{2^k+1}+\alpha_{2^k+2}+\cdots+\alpha_{2^{k+1}}}{2^k}}{2} \geq \frac{\sqrt[2^k]{\alpha_1\alpha_2\cdots\alpha_{2^k}}+\sqrt[2^k]{\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}}}{2}. \quad \textbf{(3)}$$

Επειδή όπως δείξαμε η ανισότητα αριθμητικού-γεωμετρικού μέσου ισχύει για δύο αριθμούς (εδώ μπορούμε να πάρουμε τους $\sqrt[2^k]{\alpha_1\alpha_2\cdots\alpha_{2^k}}$ και $\sqrt[2^k]{\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}}$), θα έχουμε:

$$\frac{\sqrt[2^k]{\alpha_1\alpha_2\cdots\alpha_{2^k}}+\sqrt[2^k]{\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}}}{2} \geq \sqrt{\sqrt[2^k]{\alpha_1\alpha_2\cdots\alpha_{2^k}}\sqrt[2^k]{\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}}} =$$
$$= \sqrt{\sqrt[2^k]{\alpha_1\alpha_2\cdots\alpha_{2^k}\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}}} = \sqrt[2^{k+1}]{\alpha_1\alpha_2\cdots\alpha_{2^k}\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}} \quad \textbf{(4)}$$

Από τις σχέσεις (2), (3) και (4) προκύπτει ότι

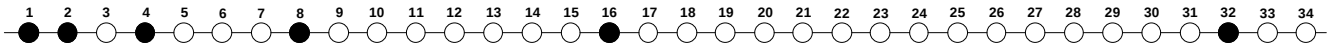
$$\frac{\alpha_1+\alpha_2+\cdots+\alpha_{2^k}+\alpha_{2^k+1}+\alpha_{2^k+2}+\cdots+\alpha_{2^{k+1}}}{2^{k+1}} \geq \sqrt[2^{k+1}]{\alpha_1\alpha_2\cdots\alpha_{2^k}\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}} \quad \textbf{(5)}$$

δηλαδή η ανισότητα ισχύει και για $n=2^{k+1}$. Με βάση την αρχή της μαθηματικής επαγωγής θα ισχύει για κάθε θετικό ακέραιο n ο οποίος είναι δύναμη του 2.
Σημειώνουμε εδώ πως για να ισχύει ως ισότητα η σχέση (3) θα πρέπει

$$\frac{\alpha_1+\alpha_2+\cdots+\alpha_{2^k}}{2^k} = \sqrt[2^k]{\alpha_1\alpha_2\cdots\alpha_{2^k}} \Leftrightarrow \alpha_1=\alpha_2=\cdots=\alpha_{2^k}\left(=\sqrt[2^k]{\alpha_1\alpha_2\cdots\alpha_{2^k}}\right) \text{ και}$$
$$\frac{\alpha_{2^k+1}+\alpha_{2^k+2}+\cdots+\alpha_{2^{k+1}}}{2^k} = \sqrt[2^k]{\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}} \Leftrightarrow$$
$$\Leftrightarrow \alpha_{2^k+1}=\alpha_{2^k+2}=\cdots=\alpha_{2^{k+1}}\left(=\sqrt[2^k]{\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}}\right).$$

Επίσης, για να ισχύει ως ισότητα η σχέση (4) θα πρέπει $\sqrt[2^k]{\alpha_1\alpha_2\cdots\alpha_{2^k}} = \sqrt[2^k]{\alpha_{2^k+1}\alpha_{2^k+2}\cdots\alpha_{2^{k+1}}}$.

Επομένως για να ισχύει ως ισότητα η σχέση (5) θα πρέπει να έχουμε $\alpha_1 = \alpha_2 = \cdots = \alpha_{2^k} = \alpha_{2^k+1} = \\ = \alpha_{2^k+2} = \cdots = \alpha_{2^{k+1}}$.
Τι γίνεται όμως για εκείνα τα n που δεν είναι δυνάμεις του 2; Αν παρατηρήσουμε το επόμενο σχήμα, θα διαπιστώσουμε ότι δημιουργούνται κενά (άσπρες μπάλλες) μεταξύ των θετικών ακεραίων. Σ' αυτά τα κενά δεν γνωρίζουμε ακόμη αν ισχύει η ανισότητα αριθμητικού-γεωμετρικού μέσου.



Σχήμα 13

Θα πάμε ανάποδα: Θα αποδείξουμε ότι αν η ανισότητα αριθμητικού-γεωμετρικού μέσου ισχύει για κάποιον θετικό ακέραιο $n > 2$, τότε θα ισχύει και για τον προηγούμενό του $n-1$. Έτσι, ξέροντας ότι ισχύει για π.χ. $n = 16$ θα ισχύει και για $n = 15$, αλλά και για $n = 14$ κ.ο.κ., κλείνοντας έτσι τα κενά στην απόδειξη. (Είναι προφανές ότι για κάθε θετικό ακέραιο n υπάρχει δύναμη του 2 που τον υπερβαίνει. Π.χ. από την ανισότητα Bernoulli παίρνουμε $2^n = (1+1)^n \geq 1 + n > n$).
Υποθέτουμε ότι η ανισότητα ισχύει για οποιουσδήποτε $n > 2$ μη αρνητικούς πραγματικούς αριθμούς. Επίσης ισχύει ως ισότητα μόνο στην περίπτωση που όλοι οι αριθμοί είναι ίσοι.
Θεωρούμε τώρα $n-1$ το πλήθος μη αρνητικούς αριθμούς $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$. Οι αριθμοί $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ και $\sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}}$ είναι n το πλήθος. Εφόσον η ανισότητα ισχύει για n αριθμούς, θα έχουμε

$$\frac{\alpha_1+\alpha_2+\cdots+\alpha_{n-1}+\sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}}}{n} \geq \sqrt[n]{\alpha_1\alpha_2\cdots\alpha_{n-1}\sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}}} \Leftrightarrow$$

$$\Leftrightarrow \frac{\alpha_1+\alpha_2+\cdots+\alpha_{n-1}+\sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}}}{n} \geq \sqrt[n]{\sqrt[n-1]{(\alpha_1\alpha_2\cdots\alpha_{n-1})^{n-1}}\cdot\sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}}} =$$

$$= \sqrt[n]{\sqrt[n-1]{(\alpha_1\alpha_2\cdots\alpha_{n-1})^{n}}} = \sqrt[n(n-1)]{(\alpha_1\alpha_2\cdots\alpha_{n-1})^{n}} = \sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}} \Leftrightarrow$$

$$\Leftrightarrow \alpha_1+\alpha_2+\cdots+\alpha_{n-1}+\sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}} \geq n\sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}} \Leftrightarrow$$

$$\Leftrightarrow \alpha_1+\alpha_2+\cdots+\alpha_{n-1} \geq (n-1)\sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}} \Leftrightarrow$$

$$\Leftrightarrow \frac{\alpha_1+\alpha_2+\cdots+\alpha_{n-1}}{n-1} \geq \sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}}.$$

Επισημαίνουμε εδώ πως η σχέση ισχύει ως ισότητα μόνον όταν $\alpha_1 = \alpha_2 = \cdots = \alpha_{n-1} = \sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}}$.
Η απόδειξη ολοκληρώθηκε. ■

ΑΛΥΤΗ ΑΣΚΗΣΗ

105. Στην προηγούμενη απόδειξη και συγκεκριμένα στην απόδειξη του βήματος από n σε $n-1$, χρησιμοποιήσαμε τον γεωμετρικό μέσο $\sqrt[n-1]{\alpha_1\alpha_2\cdots\alpha_{n-1}}$ των αριθμών $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$. Δείξτε ότι αν αντί του γεωμετρικού μέσου χρησιμοποιήσουμε τον αριθμητικό μέσο $\dfrac{\alpha_1+\alpha_2+\cdots+\alpha_{n-1}}{n-1}$ αυτών, τότε το επιχείρημα εξακολουθεί να δουλεύει.

2η Απόδειξη: Υποθέτουμε όπως και προηγουμένως ότι $\alpha_i > 0$, για κάθε $i = 1, 2, \ldots, n$. Πρώτα, αποδεικνύουμε επαγωγικά τον επόμενο ισχυρισμό:
Ισχυρισμός: Έστω $x_1, x_2, \ldots, x_n > 0$, έτσι ώστε $x_1x_2\cdots x_n = 1$. Τότε $x_1 + x_2 + \cdots + x_n \geq n$. Μάλιστα, ισχύει ισότητα αν και μόνον αν $x_1 = x_2 = \cdots = x_n = 1$.
Για $n = 1$ έχουμε $x_1 = 1 \geq 1$.
Υποθέτουμε ότι η ανισότητα ισχύει για n θετικούς αριθμούς και ότι ισχύει ως ισότητα αν και μόνον αν οι αριθμοί αυτοί είναι ίσοι (με τη μονάδα).
Έστω τώρα $x_1, x_2, \ldots, x_n, x_{n+1} > 0$, έτσι ώστε $x_1x_2\cdots x_nx_{n+1} = 1$. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $x_1 \leq x_2 \leq \cdots \leq x_n \leq x_{n+1}$. Τότε $x_{n+1} \geq 1$. Πράγματι, αν όλοι οι αριθμοί

$x_1, x_2, \ldots, x_n, x_{n+1}$ ήσαν μικρότεροι της μονάδας, τότε και το γινόμενό τους θα ήταν μικρότερο του 1. Ανάλογα προκύπτει ότι $x_1 \leq 1$.
Η σχέση $x_1x_2\cdots x_nx_{n+1} = 1$ γράφεται $(x_1x_{n+1})x_2\cdots x_n = 1$. (Έχουμε αντικαταστήσει τους $n+1$ αριθμούς $x_1, x_2, \ldots, x_n, x_{n+1}$ με τους n αριθμούς $(x_1x_{n+1}), x_2, \ldots, x_n$, θεωρώντας το γινόμενο x_1x_{n+1} ως έναν αριθμό). Από την επαγωγική υπόθεση προκύπτει ότι $(x_1x_{n+1}) + x_2 + \cdots + x_n \geq n$, με ισότητα αν και μόνον αν $(x_1x_{n+1}) = x_2 = \cdots = x_n = 1$. Παρατηρούμε ότι $x_1 + x_{n+1} \geq x_1x_{n+1} + 1 \Leftrightarrow x_{n+1}(1-x_1) + x_1 - 1 = (x_{n+1}-1)(1-x_1) \geq 0$, η οποία ισχύει γιατί $x_{n+1} \geq 1$ και $x_1 \leq 1$.
Επομένως $x_1 + x_2 + \cdots + x_n + x_{n+1} = (x_1 + x_{n+1}) + x_2 + \cdots + x_n \geq x_1x_{n+1} + 1 + x_2 + \cdots + x_n \geq n+1$. Ισότητα θα προκύψει αν έχουμε $(x_1x_{n+1}) + x_2 + \cdots + x_n = n \Leftrightarrow (x_1x_{n+1}) = x_2 = \cdots = x_n = 1$ και $(1-x_1)(x_{n+1}-1) = 0 \Leftrightarrow x_1 = 1$ ή $x_{n+1} = 1$. Στη δεύτερη περίπτωση, εφόσον $x_1x_{n+1} = 1$ παίρνουμε και $x_1 = x_{n+1} = 1$.
Προχωράμε τώρα στην απόδειξη της ανισότητας αριθμητικού-γεωμετρικού μέσου.
Θέτουμε $x_i = \dfrac{\alpha_i}{\sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}}$, για κάθε $i = 1, 2, \ldots, n$. Παρατηρούμε ότι $x_1x_2\cdots x_n = \dfrac{\alpha_1\alpha_2\cdots\alpha_n}{(\sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n})^n} = 1$.
Με βάση τον ισχυρισμό που αποδείξαμε θα έχουμε: $x_1+x_2+\cdots+x_n \geq n \Leftrightarrow \dfrac{\alpha_1}{\sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}} + \dfrac{\alpha_2}{\sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}} + \cdots + \dfrac{\alpha_n}{\sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}} \geq n \Leftrightarrow \dfrac{\alpha_1+\alpha_2+\cdots+\alpha_n}{n} \geq \sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}$.
Η ισότητα ισχύει αν και μόνον αν $x_1 = x_2 = \cdots = x_n = 1 \Leftrightarrow \dfrac{\alpha_1}{\sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}} = \dfrac{\alpha_2}{\sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}} = \cdots = \dfrac{\alpha_n}{\sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}} = 1 \Leftrightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_n = \sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}$. ■

3η Απόδειξη: Εδώ θα χρησιμοποιήσουμε την ανισότητα Bernoulli. Θέτουμε $A_k = \dfrac{\alpha_1+\alpha_2+\cdots+\alpha_k}{k}$, για κάθε $k = 1, 2, \ldots, n$. Προφανώς $A_k > 0$ (εφόσον, όπως και προηγουμένως έχουμε υποθέσει ότι οι αριθμοί $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι θετικοί) και $kA_k = \alpha_1 + \alpha_2 + \cdots + \alpha_k$, για κάθε $k = 1, 2, \ldots, n$.
Παρατηρούμε ότι για κάθε $k = 1, 2, \ldots, n-1$ έχουμε:

$$\frac{A_{k+1}^{k+1}}{A_k^k} = \frac{A_{k+1}^{k+1}}{A_k^{k+1}} \cdot A_k = \frac{\left(\dfrac{\alpha_1+\alpha_2+\cdots+\alpha_k+\alpha_{k+1}}{k+1}\right)^{k+1}}{A_k^{k+1}} A_k = \left(\frac{kA_k+\alpha_{k+1}}{(k+1)A_k}\right)^{k+1} A_k =$$
$$= \left(\frac{(k+1)A_k+\alpha_{k+1}-A_k}{(k+1)A_k}\right)^{k+1} A_k = \left(1+\frac{\alpha_{k+1}-A_k}{(k+1)A_k}\right)^{k+1} A_k.$$

Αν $\dfrac{\alpha_{k+1}-A_k}{(k+1)A_k} \leq -1$, τότε $\alpha_{k+1}-A_k \leq -(k+1)A_k \Leftrightarrow \alpha_{k+1} \leq -kA_k < 0$, άτοπο. Επομένως $\dfrac{\alpha_{k+1}-A_k}{(k+1)A_k} > -1$ και μπορούμε να εφαρμόσουμε την ανισότητα Bernoulli: $\left(1+\dfrac{\alpha_{k+1}-A_k}{(k+1)A_k}\right)^{k+1} \geq 1 + (k+1)\dfrac{\alpha_{k+1}-A_k}{(k+1)A_k} = 1 + \dfrac{\alpha_{k+1}-A_k}{A_k} = \dfrac{A_k+\alpha_{k+1}-A_k}{A_k} = \dfrac{\alpha_{k+1}}{A_k}$. Επομένως $\dfrac{A_{k+1}^{k+1}}{A_k^k} \geq \dfrac{\alpha_{k+1}}{A_k} A_k = \alpha_{k+1}$.
Εφαρμόζουμε την προηγούμενη ανισότητα για κάθε $k = 1, 2, \ldots, n-1$ και με δεδομένο ότι $A_1 = \dfrac{\alpha_1}{1} = \alpha_1$, παίρνουμε: $A_n^n = \dfrac{A_n^n}{A_{n-1}^{n-1}} \cdot \dfrac{A_{n-1}^{n-1}}{A_{n-2}^{n-2}} \cdots \dfrac{A_3^3}{A_2^2} \cdot \dfrac{A_2^2}{A_1} A_1 \geq \alpha_n\alpha_{n-1}\cdots\alpha_3\alpha_2\alpha_1$, απ΄ όπου προκύπτει

$$A_n \geq \sqrt[n]{\alpha_1\alpha_2\cdots\alpha_{n-1}\alpha_n}.$$

Σημειώνουμε ότι για να προκύψει ισότητα θα πρέπει στην ανισότητα Bernoulli $\left(1+\dfrac{\alpha_{k+1}-A_k}{(k+1)A_k}\right)^{k+1} \geq 1 + (k+1)\dfrac{\alpha_{k+1}-A_k}{(k+1)A_k}$ να έχουμε $\alpha_{k+1} = A_k$, για κάθε $k = 1, 2, \ldots, n-1$. Άρα $\alpha_2 = A_1 = \alpha_1$, $\alpha_3 = A_2 = \dfrac{2\alpha_1}{2} = \alpha_1$ κ.ο.κ. Δηλαδή $\alpha_1 = \alpha_2 = \cdots = \alpha_n$. ■

4η Απόδειξη: (Η απλούστερη γνωστή) Έστω $A = \dfrac{\alpha_1+\alpha_2+\cdots+\alpha_n}{n}$. Αν $\alpha_1 = \alpha_2 = \cdots = \alpha_n (= A)$, τότε $A = \sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}$.

Έστω ότι κάποιος α_i είναι μεγαλύτερος του A. Τότε θα υπάρχει κάποιος $\alpha_j < A$. Γιατί, σε αντίθετη περίπτωση θα είχαμε $\alpha_1+\alpha_2+\cdots+\alpha_n > nA \Rightarrow A = \dfrac{\alpha_1+\alpha_2+\cdots+\alpha_n}{n} > A$, άτοπο.
Έστω $\alpha_i = A+x$ και $\alpha_j = A-y$, όπου $x, y > 0$. Αντικαθιστούμε το α_i με το $\alpha_i' = A$ και το α_j με το $\alpha_j' = A+x-y$. Παρατηρούμε ότι $\alpha_i'+\alpha_j' = 2A+x-y = (A+x)+(A-y) = \alpha_i+\alpha_j$. Επομένως το άθροισμα και άρα ο αριθμητικός μέσος των αριθμών $\alpha_1, \alpha_2, \ldots, \alpha_i', \ldots, \alpha_j', \ldots, \alpha_n$ παραμένει ο ίδιος. Από την άλλη μεριά όμως, παρατηρούμε ότι $\alpha_i\alpha_j = (A+x)(A-y) = A^2+(x-y)A-xy \underset{xy>0}{<} A^2+(x-y)A = A(A+x-y) = \alpha_i'\alpha_j'$. Επομένως ο γεωμετρικός μέσος των αριθμών $\alpha_1, \alpha_2, \ldots, \alpha_i', \ldots, \alpha_j', \ldots, \alpha_n$ είναι μεγαλύτερος του αρχικού γεωμετρικού μέσου. Αν συνεχίσουμε κατ΄ αυτόν τον τρόπο, θα αυξάνουμε συνεχώς τον γεωμετρικό μέσο, ενώ ο αριθμητικός μέσος θα παραμένει ο ίδιος. Επιπροσθέτως, με την αντικατάσταση του α_i από το $\alpha_i' = A$ αυξάνουμε το πλήθος των αριθμών που είναι ίσοι με A, τουλάχιστον κατά έναν. (Μπορεί και ο $\alpha_j' = A+x-y$ να γίνει ίσος με A, αν $x = y$). Το βέβαιο είναι ότι αυτή η διαδικασία κάποτε θα σταματήσει, όταν φυσικά όλοι οι αριθμοί γίνουν ίσοι με A, οπότε και θα έχουμε ισότητα μεταξύ αριθμητικού και γεωμετρικού μέσου. ■

Παρατήρηση: Και στην προηγούμενη 4η απόδειξη υποκρύπτεται επαγωγή ως προς το πλήθος των $\alpha_1, \alpha_2, \ldots, \alpha_n$ που δεν είναι ίσοι με A.

ΛΥΜΕΝΕΣ ΑΣΚΗΣΕΙΣ

Άσκηση 119. Αν $\alpha_1, \alpha_2, \ldots, \alpha_n > 0$ να δείξετε ότι $\dfrac{\alpha_1}{\alpha_2}+\dfrac{\alpha_2}{\alpha_3}+\cdots+\dfrac{\alpha_{n-1}}{\alpha_n}+\dfrac{\alpha_n}{\alpha_1} \geq n$.

Απόδειξη: Σύμφωνα με την ανισότητα αριθμητικού-γεωμετρικού μέσου έχουμε:
$\dfrac{\dfrac{\alpha_1}{\alpha_2}+\dfrac{\alpha_2}{\alpha_3}+\cdots+\dfrac{\alpha_{n-1}}{\alpha_n}+\dfrac{\alpha_n}{\alpha_1}}{n} \geq \sqrt[n]{\dfrac{\cancel{\alpha_1}}{\cancel{\alpha_2}}\cdot\dfrac{\cancel{\alpha_2}}{\cancel{\alpha_3}}\cdots\dfrac{\cancel{\alpha_{n-1}}}{\cancel{\alpha_n}}\cdot\dfrac{\cancel{\alpha_n}}{\cancel{\alpha_1}}} = \sqrt[n]{1} = 1$, απ΄ όπου προκύπτει η αποδεικτέα σχέση. ■

Άσκηση 120. Αποδείξτε ότι για κάθε $n \geq 3$ ισχύει η σχέση: $1+\dfrac{1}{2}+\dfrac{1}{3}+\cdots+\dfrac{1}{n} < n-\dfrac{n-1}{\sqrt[n-1]{n}}$.

Απόδειξη: Η σχέση $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} < n-\dfrac{n-1}{\sqrt[n-1]{n}}$ ισοδύναμα γράφεται $\dfrac{n-1}{\sqrt[n-1]{n}} < n-\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}\right) =$
$= 1-1+\left(1-\dfrac{1}{2}\right)+\left(1-\dfrac{1}{3}\right)+\cdots+\left(1-\dfrac{1}{n}\right) = \dfrac{1}{2}+\dfrac{2}{3}+\cdots+\dfrac{n-1}{n}$.
Από την ανισότητα αριθμητικού-γεωμετρικού μέσου παίρνουμε:
$$\frac{\frac{1}{2}+\frac{2}{3}+\cdots+\frac{n-1}{n}}{n-1} > \sqrt[n-1]{\frac{\cancel{1}}{\cancel{2}}\cdot\frac{\cancel{2}}{\cancel{3}}\cdots\frac{\cancel{n-1}}{n}} = \frac{1}{\sqrt[n-1]{n}} \Leftrightarrow \frac{n-1}{\sqrt[n-1]{n}} < \frac{1}{2}+\frac{2}{3}+\cdots+\frac{n-1}{n}.$$ ■

Άσκηση 121. Αποδείξτε ότι για κάθε $n \geq 2$ ισχύει η σχέση: $n\left(\sqrt[n]{n+1}-1\right) < 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$.
Απόδειξη: Η σχέση $n\left(\sqrt[n]{n+1}-1\right) < 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$ ισοδύναμα γράφεται $n\sqrt[n]{n+1} < 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}+n = (1+1)+\left(\frac{1}{2}+1\right)+\left(\frac{1}{3}+1\right)+\cdots+\left(\frac{1}{n}+1\right) = \frac{2}{1}+\frac{3}{2}+\frac{4}{3}+\cdots+\frac{n+1}{n}$.
Από την ανισότητα αριθμητικού-γεωμετρικού μέσου παίρνουμε:
$$\frac{\frac{2}{1}+\frac{3}{2}+\frac{4}{3}\cdots+\frac{n+1}{n}}{n} > \sqrt[n]{\frac{\cancel{2}}{1}\cdot\frac{\cancel{3}}{\cancel{2}}\cdot\frac{\cancel{4}}{\cancel{3}}\cdots\frac{n+1}{\cancel{n}}} = \sqrt[n]{n+1} \Leftrightarrow n\sqrt[n]{n+1} < \frac{2}{1}+\frac{3}{2}+\frac{4}{3}+\cdots+\frac{n+1}{n}.$$ ■

ΑΛΥΤΕΣ ΑΣΚΗΣΕΙΣ

106. Δείξτε ότι $(n!)^3 < n^n\left(\dfrac{n+1}{2}\right)^{2n}$ για κάθε $n = 2, 3, \ldots$

107. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύει: $\sqrt[n]{(3n)!} < \dfrac{3n(3n+1)^2}{4}$.

Πρόταση Γ΄.20. Έστω $A \subseteq \mathbb{Z}_{\geq n_0}$ και m σταθερός θετικός ακέραιος. Υποθέτουμε ότι:
(i) $n_0, n_0+1, n_0+2, \ldots, n_0+m-1 \in A$ και

(ii) αν m διαδοχικοί ακέραιοι $n, n+1, n+2, \ldots, n+m-1 \in \mathrm{A}$, τότε $n+m \in \mathrm{A}$.
Τότε $\mathrm{A} = \mathbb{Z}_{\geq n_0}$.
Απόδειξη: Έστω $\mathrm{A} \subsetneq \mathbb{Z}_{\geq n_0}$. Τότε το $\mathrm{A}' = \mathbb{Z}_{\geq n_0} \setminus \mathrm{A}$ είναι μη κενό και κάτω φραγμένο. Μάλιστα, είναι κάτω φραγμένο από το $n_0 + m - 1$, γιατί δεν υπάρχουν ακέραιοι μεταξύ διαδοχικών ακεραίων και n_0, n_0+1, $n_0+2, \ldots, n_0+m-1 \notin \mathrm{A}'$. Έστω $\mu = \min \mathrm{A}'$. Τότε $n_0 + m - 1 < \mu \Rightarrow n_0 + m - 1 \leq \mu - 1 \Leftrightarrow n_0 \leq \mu - m$. Οι m διαδοχικοί ακέραιοι $\mu - m, \mu - m + 1, \mu - m + 2 \ldots, \mu - 1$ ανήκουν στο A, γιατί $n_0 \leq \mu - m \leq \mu - 1 <$ $< \mu = \min \mathrm{A}'$. Από τη συνθήκη (ii) προκύπτει ότι και $\mu = (\mu - 1) + 1 \in \mathrm{A}$, άτοπο. Άρα $\mathrm{A}' = \varnothing$, δηλαδή $\mathrm{A} = \mathbb{Z}_{\geq n_0}$. ■
Η παραπάνω πρόταση μας επιτρέπει να εφαρμόζουμε μια παραλλαγή της μαθηματικής επαγωγής.

Πόρισμα Γ΄.21. Έστω $p(n)$ ένας προτασιακός τύπος. Υποθέτουμε τα εξής:
1ο : Η πρόταση $p(n_0)$ είναι αληθής.
2ο : Αν $p(n), p(n+1), \ldots, p(n+m-1)$ είναι αληθείς, τότε και η $p(n+m)$ είναι αληθής.
Τότε η πρόταση $p(n)$ είναι αληθής για κάθε ακέραιο $n \geq n_0$.
Απόδειξη: Έστω $\mathrm{A} = \{n \in \mathbb{Z}_{\geq n_0} \mid \text{η } p(n) \text{ είναι αληθής}\}$. Εφόσον η $p(n_0)$ είναι αληθής, έχουμε $n_0 \in \mathrm{A}$. Αν τώρα $n, n+1, n+2, \ldots, n+m-1 \in \mathrm{A}$, τότε $p(n), p(n+1), \ldots, p(n+m-1)$ είναι αληθείς. Από την υπόθεσή μας προκύπτει ότι και η $p(n+m)$ είναι αληθής. Άρα $n+m \in \mathrm{A}$. Με βάση την προηγούμενη πρόταση $\mathrm{A} = \mathbb{Z}_{\geq n_0}$, δηλαδή η $p(n)$ είναι αληθής για κάθε $n \geq n_0$. ■

Η επόμενη άσκηση αφορά τους περίφημους **αριθμούς Fibonacci**.

Άσκηση 122. (Ακολουθία Fibonacci) Θεωρούμε την ακολουθία $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$ Παρατηρούμε ότι κάθε όρος της ακολουθίας αυτής, από τον 3ο και μετά, ισούται με το άθροισμα των δύο προηγουμένων του. Δηλαδή, αν f_n είναι ο $n-$στος όρος της ακολουθίας αυτής, τότε έχουμε $f_{n+2} = f_{n+1} + f_n$. Δείξτε ότι ο $n-$στος όρος f_n δίνεται από τον τύπο

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Απόδειξη: Για $n = 1$ έχουμε: $\frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right) - \left(\frac{1-\sqrt{5}}{2} \right) \right) = \frac{1}{\sqrt{5}} \cdot \frac{(1+\sqrt{5}) - (1-\sqrt{5})}{2} = \frac{2\sqrt{5}}{2\sqrt{5}} =$
$= 1 = f_1$. Άρα η πρόταση ισχύει για $n = 1$.
Για $n = 2$ έχουμε: $\frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^2 - \left(\frac{1-\sqrt{5}}{2} \right)^2 \right) = \frac{1}{\sqrt{5}} \left(\frac{6+2\sqrt{5}}{4} - \frac{6-2\sqrt{5}}{4} \right) = \frac{1}{\sqrt{5}} \cdot \frac{4\sqrt{5}}{4} = 1 =$
$= f_2$. Άρα η πρόταση ισχύει για $n = 2$.
Υποθέτουμε ότι η πρόταση ισχύει για n και $n+1$, δηλαδή $f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$ και
$f_{n+1} = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right)$. Θα αποδείξουμε ότι ισχύει και για $n+2$.
Έχουμε:

$$f_{n+2} = f_{n+1} + f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right) + \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right) =$$
$$= \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} + \left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^n \right) =$$
$$= \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{1+\sqrt{5}}{2} + 1 \right) - \left(\frac{1-\sqrt{5}}{2} \right)^n \left(\frac{1-\sqrt{5}}{2} + 1 \right) \right) =$$

$$= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n \cdot \frac{3+\sqrt{5}}{2} - \left(\frac{1-\sqrt{5}}{2}\right)^n \cdot \frac{3-\sqrt{5}}{2}\right) =$$
$$= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n \cdot \frac{6+2\sqrt{5}}{4} - \left(\frac{1-\sqrt{5}}{2}\right)^n \cdot \frac{6-2\sqrt{5}}{4}\right) =$$
$$= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n \left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^n \left(\frac{1-\sqrt{5}}{2}\right)^2\right) = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+2}\right).$$

Επομένως η πρόταση ισχύει και για $n+2$. Με βάση το προηγούμενο πόρισμα, ισχύει για κάθε θετικό ακέραιο n. ■

Φυσικά δεν είναι δυνατόν να μαντέψει κανείς τον παραπάνω περίεργο τύπο για τους αριθμούς Fibonacci. Υπάρχουν μέθοδοι, για παράδειγμα μέσω διαγωνοποίησης πινάκων ή δυναμοσειρών, οι οποίες οδηγούν σ᾽ αυτό το αποτέλεσμα.

ΛΥΜΕΝΕΣ ΑΣΚΗΣΕΙΣ

Άσκηση 123. Δείξτε ότι για κάθε δύο θετικούς ακεραίους m, n με $n \geq 2$, ισχύει η σχέση: $f_{m+n} = f_m f_{n-1} + f_{m+1} f_n$.

Απόδειξη: Αποδεικνύουμε την παραπάνω σχέση με επαγωγή ως προς m.

Για $m = 1$ και οποιονδήποτε θετικό ακέραιο $n \geq 2$, έχουμε: $f_{m+n} = f_{n+1} = f_{n-1} + f_n = 1 \cdot f_{n-1} + 1 \cdot f_n = f_1 f_{n-1} + f_2 f_n \underset{m=1}{=} f_m f_{n-1} + f_{m+1} f_n$.

Υποθέτουμε ότι $f_{m+n} = f_m f_{n-1} + f_{m+1} f_n$ για κάποιο θετικό ακέραιο m και **για όλους** τους ακεραίους $n \geq 2$. Θα αποδείξουμε ότι $f_{(m+1)+n} = f_{m+1} f_{n-1} + f_{m+2} f_n$ για όλους τους ακεραίους $n \geq 2$.

Πράγματι, $f_{(m+1)+n} = f_{m+(n+1)} = f_m f_{(n+1)-1} + f_{m+1} f_{n+1} = f_m f_n + f_{m+1} f_{n+1}$, λόγω της επαγωγικής υπόθεσης. Επίσης, $f_{n+1} = f_n + f_{n-1}$ και συνεπώς $f_m f_n + f_{m+1} f_{n+1} = = f_m f_n + f_{m+1} f_n + f_{m+1} f_{n-1} = f_{m+1} f_{n-1} + (f_m + f_{m+1}) f_n = f_{m+1} f_{n-1} + f_{m+2} f_n$. ■

Άσκηση 124. Δίνεται η ακολουθία των αριθμών -3, 15, -21, 99, -213, 795, -2061, 6819, -19173, ... Αν α_n είναι γενικός όρος της ακολουθίας, τότε έχουμε $\alpha_1 = -3$, $\alpha_2 = 15$, $\alpha_3 = -21$ και κάθε άλλος όρος δίνεται συναρτήσει των τριών προηγούμενών του από τη σχέση: $\alpha_{n+3} = 6\alpha_n + 5\alpha_{n+1} - 2\alpha_{n+2}$.

Θα αποδείξουμε ότι

$$\alpha_n = 2(-1)^n + 2^n + (-3)^n$$

για κάθε $n = 1, 2, 3, ...$

Απόδειξη: Αρχικώς επαληθεύουμε τον τύπο για $n = 1, n = 2$ και $n = 3$. (Η εκτέλεση των πράξεων είναι θέμα ρουτίνας και παραλείπεται. Ο δύσπιστος αναγνώστης μπορεί να κάνει μόνος του την επαλήθευση).

Στη συνέχεια υποθέτουμε ότι ο τύπος ισχύει για n, $n+1$ και $n+2$. Θα αποδείξουμε ότι ισχύει και για $n+3$. Έχουμε λοιπόν τις σχέσεις:

$$\alpha_n = 2(-1)^n + 2^n + (-3)^n$$
$$\alpha_{n+1} = 2(-1)^{n+1} + 2^{n+1} + (-3)^{n+1}$$
$$\text{και } \alpha_{n+2} = 2(-1)^{n+2} + 2^{n+2} + (-3)^{n+2}.$$

Τότε θα έχουμε: $\alpha_{n+3} = 6\alpha_n + 5\alpha_{n+1} - 2\alpha_{n+2} = 6\big(2(-1)^n + 2^n + (-3)^n\big) + 5\big(2(-1)^{n+1} + 2^{n+1} + (-3)^{n+1}\big) - 2\big(2(-1)^{n+2} + 2^{n+2} + (-3)^{n+2}\big) = 12(-1)^n + 6 \cdot 2^n + 6(-3)^n + 10(-1)^{n+1} + 5 \cdot 2^{n+1} + 5(-3)^{n+1} - 4(-1)^{n+2} - 2^{n+3} - 2(-3)^{n+2} = (-1)^n\big(12 + 10(-1) - 4(-1)^2\big) + 2^n\big(6 + 5 \cdot 2 - 2^3\big) + (-3)^n\big(6 + 5(-3) - 2(-3)^2\big) = (-1)^n(12 - 10 - 4) + 2^n(6 + 10 - 8) + (-3)^n(6 - 15 - 18) = -2(-1)^n + 8 \cdot 2^n - 27(-3)^n = 2(-1)^3(-1)^n + 2^3 \cdot 2^n + (-3)^3 \cdot (-3)^n = 2(-1)^{n+3} + 2^{n+3} + (-3)^{n+3}$.

Εφόσον λοιπόν ο τύπος ισχύει για $n = 1$, $n = 2$ και $n = 3$, με βάση τα προηγούμενα θα ισχύει και για $n = 4$. Εφόσον ισχύει για $n = 2$, $n = 3$ και για $n = 4$, θα ισχύει και για $n = 5$. Προφανώς η διαδικασία αυτή δεν σταματά και κατά συνέπεια η απόδειξη θεωρείται πλήρης. ■

Άσκηση 125. Δίνεται η ακολουθία με γενικό όρο $\alpha_n = (3+\sqrt{5})^n + (3-\sqrt{5})^n$, $n = 1, 2, 3, \ldots$ Να αποδείξετε ότι ο α_n είναι ακέραιος και μάλιστα πολλαπλάσιο του 2^n.

Απόδειξη: Για $n = 1$ έχουμε $\alpha_1 = (3 + \sqrt{5}) + (3 - \sqrt{5}) = 6 = 3 \cdot 2^1$. Για $n = 2$ έχουμε $\alpha_2 = = (3 + \sqrt{5})^2 + (3 - \sqrt{5})^2 = 9 + 6\sqrt{5} + 5 + 9 - 6\sqrt{5} + 5 = 28 = 7 \cdot 2^2$. Άρα η πρόταση είναι αληθής για $n = 1$ και $n = 2$.

Υποθέτουμε ότι οι αριθμοί $\alpha_n = (3+\sqrt{5})^n + (3-\sqrt{5})^n$ και $\alpha_{n+1} = (3+\sqrt{5})^{n+1} + (3-\sqrt{5})^{n+1}$ είναι ακέραια πολλαπλάσια των 2^n και 2^{n+1}, αντίστοιχα. Παρατηρούμε ότι:

$$\begin{aligned}(3+\sqrt{5})\alpha_{n+1} = (3+\sqrt{5})^{n+2} + (3+\sqrt{5})(3-\sqrt{5})^{n+1} &= (3+\sqrt{5})^{n+2} + \left(3^2 - (\sqrt{5})^2\right)(3-\sqrt{5})^n = \\ &= (3+\sqrt{5})^{n+2} + 4(3-\sqrt{5})^n \text{ και}\\ (3-\sqrt{5})\alpha_{n+1} = (3-\sqrt{5})(3+\sqrt{5})^{n+1} + (3-\sqrt{5})^{n+2} &= \left(3^2 - (\sqrt{5})^2\right)(3+\sqrt{5})^n + (3-\sqrt{5})^{n+2} = \\ &= 4(3+\sqrt{5})^n + (3+\sqrt{5})^{n+2}.\end{aligned}$$

Επομένως, προσθέτοντας κατά μέλη παίρνουμε: $6\alpha_{n+1} = 4\alpha_n + \alpha_{n+2} \Leftrightarrow \alpha_{n+2} = 6\alpha_{n+1} - 4\alpha_n$. Από την τελευταία σχέση προκύπτει ότι όλοι οι αριθμοί α_n είναι ακέραιοι.

Υποθέτουμε ότι το α_n είναι πολλαπλάσιο του 2^n και το α_{n+1} πολλαπλάσιο του 2^{n+1}. Τότε το $4\alpha_n = 2^2\alpha_n$ και το $6\alpha_{n+1} = 3 \cdot 2\alpha_{n+1}$ είναι πολλαπλάσια του 2^{n+2}. Επομένως το $\alpha_{n+2} = 6\alpha_{n+1} - 4\alpha_n$ είναι πολλαπλάσιο του 2^{n+2}. ■

ΑΛΥΤΕΣ ΑΣΚΗΣΕΙΣ

108. Αποδείξτε με επαγωγή τις ακόλουθες ταυτότητες μεταξύ των αριθμών Fibonacci:

1. $f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$
2. $f_2 + f_4 + f_4 + \cdots + f_{2n} = f_{2n+1} - 1$
3. $f_1 + f_3 + f_5 + \cdots + f_{2n-1} = f_{2n}$
4. $f_1 - f_2 + f_3 + \cdots + (-1)^{n+1} f_n = (-1)^{n+1} f_{n-1} + 1$, $n \geq 2$
5. $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$, $n \geq 2$
6. $f_{n+1}^2 = 4 f_n f_{n-1} + f_{n-2}^2$, $n \geq 3$
7. $f_n^2 + f_{n-1}^2 = f_{2n-1}$, $n \geq 2$
8. $f_{n+1}^2 - f_{n-1}^2 = f_{2n}$, $n \geq 2$
9. $f_{n+1}^3 + f_n^3 - f_{n-1}^3 = f_{3n}$, $n \geq 2$
10. $f_1^2 + f_2^2 + f_3^2 + \cdots + f_n^2 = f_n f_{n+1}$
11. $f_1 f_2 + f_2 f_3 + \cdots + f_{2n-1} f_{2n} = f_{2n}^2$
12. $f_1 f_2 + f_2 f_3 + \cdots + f_{2n} f_{2n+1} = f_{2n+1}^2 - 1$

109. Δίνεται η ακολουθία με γενικό όρο $\alpha_n = (3 + 3\sqrt{2})^n + (3 - 3\sqrt{2})^n$, $n = 1, 2, 3, \ldots$ Να αποδείξετε ότι ο α_n είναι ακέραιος και μάλιστα πολλαπλάσιο του 3^n.

110. Η ακολουθία των αριθμών α_n ορίζεται ως εξής: $\alpha_1 = 1$, $\alpha_2 = 3$ και $\alpha_{n+2} = 3\alpha_{n+1} + 6\alpha_n$. Να δείξετε ότι $\alpha_n = \frac{1}{\sqrt{33}}\left(\left(\frac{3+\sqrt{33}}{2}\right)^n - \left(\frac{3-\sqrt{33}}{2}\right)^n\right)$, για κάθε $n = 1, 2, 3, \ldots$

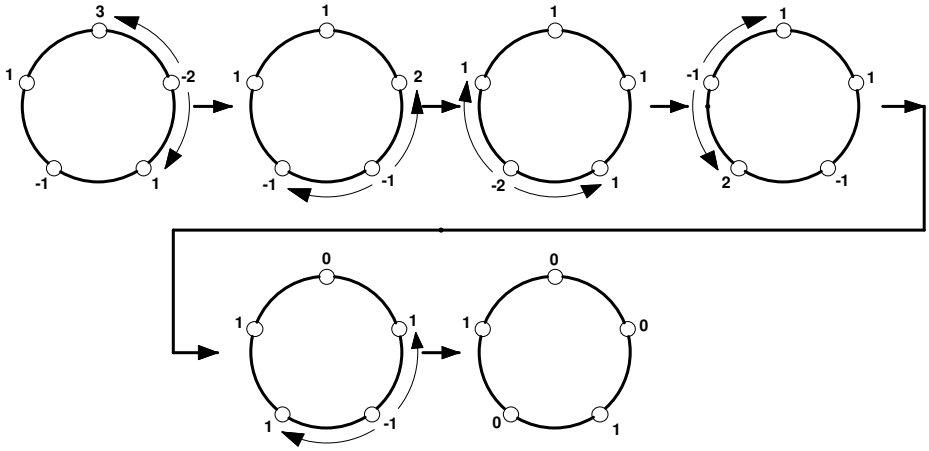
111. Δίνεται η ακολουθία των αριθμών α_n με $\alpha_1 = 7$, $\alpha_2 = -7$, $\alpha_3 = -137$ και $\alpha_{n+3} = 19\alpha_{n+1} - 30\alpha_n$. Να αποδείξετε ότι για κάθε θετικό ακέραιο n ισχύει ο τύπος: $\alpha_n = 3^{n+1} - 2 \cdot 5^n + 2^{n+2}$.

Τέλος, η επόμενη πρόταση μας παρέχει μια άλλη μορφή, ιδιαίτερα χρήσιμη και αποτελεσματική, της απόδειξης μέσω επαγωγής.

Πρόταση Γ΄.22. Έστω $\mathrm{A} \subseteq \mathbb{Z}_{\geq n_0}$. Υποθέτουμε ότι: (i) $n_0 \in \mathrm{A}$ και (ii) αν $k \in \mathrm{A}$, για κάθε $k \in \mathbb{Z}$ με $n_0 \leq k < n$, τότε και $n \in \mathrm{A}$. Τότε $\mathrm{A} = \mathbb{Z}_{\geq n_0}$.
Απόδειξη: Έστω $\mathrm{A} \subsetneq \mathbb{Z}_{\geq n_0}$. Τότε το $\mathrm{A}' = \mathbb{Z}_{\geq n_0} \setminus \mathrm{A}$ είναι μη κενό και κάτω φραγμένο. Έστω $m = \min \mathrm{A}'$. Επειδή $m \notin \mathrm{A}$ και $n_0 \in \mathrm{A}$, έπεται ότι $m > n_0$ και άρα $m - n_0 \geq 1$, ήτοι $m - 1 \geq n_0$. Επειδή $m - 1 \notin \mathrm{A}'$ έχουμε $m - 1 \in \mathrm{A}$, αλλά και $k \in \mathrm{A}$, για κάθε $k \in \mathbb{Z}$ με $n_0 \leq k \leq m - 1$, δηλαδή (εφόσον δεν υπάρχει ακέραιος μεταξύ $m - 1$ και m), για κάθε $k \in \mathbb{Z}$ με $n_0 \leq k < m$. Αλλά τότε θα έπρεπε $m \in \mathrm{A}$, άτοπο. ■

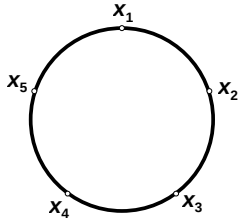
Πόρισμα Γ΄.23. Έστω $p(n)$ ένας προτασιακός τύπος. Υποθέτουμε τα εξής:
1ο : Η πρόταση $p(n_0)$ είναι αληθής.
2ο : Αν η $p(m)$ είναι αληθής για κάθε ακέραιο m, με $n_0 \leq m < n$, τότε και η $p(n)$ είναι αληθής.
Τότε η πρόταση $p(n)$ είναι αληθής για κάθε ακέραιο $n \geq n_0$.
Απόδειξη: Έστω $\mathrm{A} = \{n \in \mathbb{Z}_{\geq n_0} \mid \text{η } p(n) \text{ είναι αληθής}\}$. Εφόσον η $p(n_0)$ είναι αληθής, έχουμε $n_0 \in \mathrm{A}$. Αν τώρα $m \in \mathrm{A}$, για κάθε ακέραιο m με $n_0 \leq m < n$, τότε η $p(m)$ είναι αληθής για κάθε ακέραιο m, με $n_0 \leq m < n$. Συνεπώς και η $p(n)$ είναι αληθής, δηλαδή $n \in \mathrm{A}$. Με βάση την παραπάνω πρόταση, $\mathrm{A} = \mathbb{Z}_{n \geq n_0}$, δηλαδή η $p(n)$ είναι αληθής για κάθε $n \geq n_0$. ■

Άσκηση 126. (Διεθνής Μαθηματική Ολυμπιάδα 1986) Στην περιφέρεια κύκλου είναι τοποθετημένοι πέντε ακέραιοι αριθμοί των οποίων το άθροισμα είναι θετικό. Επιλέγουμε από αυτούς κάποιον ο οποίος είναι αρνητικός (όποιον θέλουμε, αν φυσικά υπάρχει τέτοιος), τον προσθέτουμε στους δύο γειτονικούς του και στη συνέχεια του αλλάζουμε πρόσημο. Συνεχίζουμε κατ΄ αυτόν τον τρόπο έως ότου καταλήξουμε στην περίπτωση που όλοι είναι μεγαλύτεροι ή ίσοι του μηδενός. Τότε σταματάμε. Να αποδείξετε ότι η διαδικασία αυτή κάποτε θα σταματήσει, δηλαδή σίγουρα θα καταλήξουμε κάποια στιγμή σ΄ ένα σύνολο μη αρνητικών αριθμών, ανεξάρτητα με ποιο τρόπο έχουμε επιλέξει κάθε φορά τον αρνητικό αριθμό. Ας δούμε το παράδειγμα το οποίο παριστάνεται στο επόμενο σχήμα:



Σχήμα 14

Στο σχήμα αυτό έχουμε τοποθετήσει κυκλικά τους ακεραίους 3, -2, 1, -1 και 1. Αυτοί έχουν άθροισμα $2 > 0$. Παρατηρούμε ότι η διαδικασία σταματά μετά από πέντε βήματα.
Απόδειξη: Έστω x_1, x_2, x_3, x_4, x_5 οι πέντε ακέραιοι τοποθετημένοι κυκλικά στην περιφέρεια κύκλου.



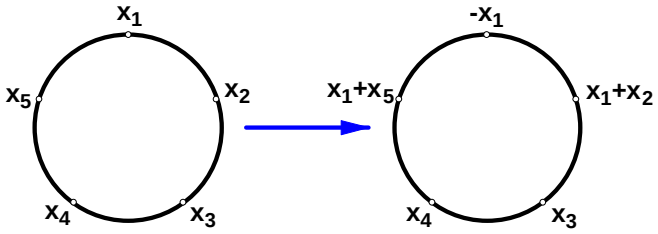
Σχήμα 15

Σε τέτοιου είδους προβλήματα προσπαθούμε να αντιστοιχίσουμε σε κάθε κατάσταση έναν μη αρνητικό ακέραιο αριθμό ο οποίος συνεχώς θα μειώνεται. Έτσι κάποια στιγμή, εφόσον ο αριθμός αυτός δεν μπορεί να «πέσει» κάτω από το μηδέν, η διαδικασία θα σταματήσει. Η εύρεση της θετικής ακέραιας ποσότητας

είναι το μεγάλο πρόβλημα. Στην περίπτωσή μας είναι η

$$\text{A} := x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + (x_1 + x_2)^2 + (x_2 + x_3)^2 + (x_3 + x_4)^2 + (x_4 + x_5)^2 + (x_5 + x_1)^2.$$

(Η πρώτη σκέψη που έκανα ήταν να προσπαθήσω να μειώσω την ποσότητα $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$, αλλά δεν δούλεψε). Με αυτόν τον τρόπο ουσιαστικά εφαρμόζουμε επαγωγή επί του A. Η ελάχιστη τιμή που μπορεί να πάρει η ποσότητα A είναι 3 (ένας ισούται με 1 και οι υπόλοιποι μηδέν-αποδείξτε το!)
Ας υποθέσουμε ότι ο x_1 είναι αρνητικός, τον οποίο προσθέτουμε στους x_5 και x_2 και μετά του αλλάζουμε πρόσημο.



Σχήμα 16

Στο παραπάνω σχήμα οι αριθμοί τώρα είναι: $-x_1, x_1+x_2, x_3, x_4$ και x_1+x_5 με άθροισμα $-x_1+(x_1+x_2)+x_3+x_4+(x_1+x_5) = x_1+x_2+x_3+x_4+x_5$, το ίδιο όπως και προηγουμένως. Η ποσότητα A όμως άλλαξε και έγινε $A' = x_1^2+(x_1+x_2)^2+x_3^2+x_4^2+(x_1+x_5)^2+(-x_1+x_1+x_2)^2+(x_1+x_2+x_3)^2+(x_3+x_4)^2+(x_4+x_1+x_5)^2+(x_1+x_5-x_1)^2 = x_1^2+(x_1+x_2)^2+x_3^2+x_4^2+(x_1+x_5)^2+x_2^2+(x_1+x_2+x_3)^2+(x_3+x_4)^2+(x_4+x_1+x_5)^2+x_5^2$. Επομένως $A-A' = \cancel{x_1^2}+\cancel{x_2^2}+\cancel{x_3^2}+\cancel{x_4^2}+\cancel{x_5^2}+\cancel{(x_1+x_2)^2}+(x_2+x_3)^2+\cancel{(x_3+x_4)^2}+(x_4+x_5)^2+\cancel{(x_5+x_1)^2}-\cancel{x_1^2}-\cancel{(x_1+x_2)^2}-\cancel{x_3^2}-\cancel{x_4^2}-\cancel{(x_1+x_5)^2}-\cancel{x_2^2}-(x_1+x_2+x_3)^2-\cancel{(x_3+x_4)^2}-(x_4+x_1+x_5)^2-\cancel{x_5^2} = (x_2+x_3)^2+(x_4+x_5)^2-(x_1+x_2+x_3)^2-(x_4+x_1+x_5)^2 = ((x_2+x_3)-(x_1+x_2+x_3))((x_2+x_3)+(x_1+x_2+x_3))+((x_4+x_5)-(x_4+x_1+x_5))((x_4+x_5)+(x_4+x_1+x_5)) = -x_1(x_1+2x_2+2x_3)-x_1(x_1+2x_4+2x_5) = -2x_1(x_1+x_2+x_3+x_4+x_5) > 0$, γιατί $x_1 < 0$ και $x_1+x_2+x_3+x_4+x_5 > 0$. Επομένως $A' < A$ και με βάση την επαγωγική υπόθεση, ξεκινώντας από τη νέα κυκλική μορφή, η διαδικασία κάποτε θα σταματήσει. ■

Γ΄.2 Το διώνυμο του Newton

Οι ταυτότητες $(\alpha+\beta)^2 = \alpha^2+2\alpha\beta+\beta^2$ και $(\alpha+\beta)^3 = \alpha^3+3\alpha^2\beta+3\alpha\beta^2+\beta^3$ μας είναι ήδη γνωστές. Με προσοχή στις πράξεις μπορεί κανείς να αποδείξει την ταυτότητα $(\alpha+\beta)^4 = \alpha^4+4\alpha^3\beta+6\alpha^2\beta^2+4\alpha\beta^3+\beta^4$ ή, αν διαθέτει περισσότερη υπομονή (!) την ταυτότητα $(\alpha+\beta)^5 = \alpha^5+5\alpha^4\beta+10\alpha^3\beta^2+10\alpha^2\beta^3+5\alpha\beta^4+\beta^5$. Γεννάται λοιπόν το ερώτημα: Υπάρχει γενικός τύπος ο οποίος να μας δίνει αμέσως το ανάπτυγμα του $(\alpha+\beta)^n$ για οποιονδήποτε (θετικό) ακέραιο n;

Ορισμός Γ΄.24. Έστω $x \in \mathbb{R}$ και k φυσικός αριθμός. Ορίζουμε:

$$\binom{x}{k} = \begin{cases} \dfrac{x(x-1)(x-2)\cdots(x-k+1)}{k!}, & \text{αν } k > 0 \\ 1, & \text{αν } k = 0. \end{cases}$$

Το σύμβολο $\binom{x}{k}$ διαβάζεται ***x* ανά *k***.

Ο παράγοντας $x-k+1$ στον αριθμητή $x(x-1)(x-2)\cdots(x-k+1)$ του συμβόλου $\binom{x}{k}$ δικαιολογείται αν παρατηρήσουμε ότι $\binom{x}{k} = \dfrac{(x-0)(x-1)(x-2)\cdots(x-(k-1))}{1\cdot 2\cdot 3\cdots k}$. Κοντολογίς, όσοι παράγοντες είναι πάνω είναι και κάτω.

Πρόταση Γ΄.25. Αν $x \notin \mathbb{N}$, τότε $\binom{x}{k} \neq 0$.

Απόδειξη: Αν $k = 0$, τότε $\binom{x}{k} = 1 \neq 0$. Έστω $k > 0$. Τότε, για να είναι $\binom{x}{k} = \dfrac{x(x-1)\cdots(x-k+1)}{k!} = 0$, θα πρέπει κάποιος από τους $x, x-1, \ldots, x-k+1$ να είναι μηδέν. Δηλαδή, $x - s = 0$, για κάποιο $s = 0, 1, \ldots, k-1$. Τότε όμως $x = s \in \mathbb{N}$, άτοπο. ■

Στα επόμενα θα ασχοληθούμε με περιπτώσεις στις οποίες το x είναι μη αρνητικός ακέραιος και γι΄ αυτό προτιμούμε το σύμβολο n αντί του x. Ας υπολογίσουμε τώρα κάποια από τα σύμβολα $\binom{n}{k}$:

(i) $\binom{6}{4} = \dfrac{6\cdot 5\cdot 4\cdot 3}{1\cdot 2\cdot 3\cdot 4} = \dfrac{\cancel{6}\cdot 5\cdot 4\cdot 3}{1\cdot \cancel{2\cdot 3}\cdot 4} = \dfrac{5\cdot \cancel{4}\cdot 3}{\cancel{4}} = 5\cdot 3 = 15.$

(ii) $\binom{7}{3} = \dfrac{7\cdot \cancel{6}\cdot 5}{\cancel{1\cdot 2\cdot 3}} = 35.$

(iii) $\binom{12}{5} = \dfrac{12\cdot 11\cdot 10\cdot 9\cdot 8}{2\cdot 3\cdot 4\cdot 5} = \dfrac{12\cdot 11\cdot \cancel{10}\cdot 9\cdot 8}{\cancel{2}\cdot 3\cdot 4\cdot \cancel{5}} = \dfrac{\cancel{12}\cdot 11\cdot 9\cdot 8}{\cancel{3\cdot 4}} = 11\cdot 72 = 792.$

Επειδή στο σύμβολο $\binom{x}{k}$ εμφανίζονται γινόμενα πολλών αριθμών, αποφεύγουμε να κάνουμε αμέσως τους πολλαπλασιασμούς αλλά προτιμούμε να απλοποιούμε πρώτα τα κλάσματα. (Όπως έχουμε μάθει να κάνουμε γενικά στα μαθηματικά).

Η επόμενη πρόταση περιγράφει μερικές από τις βασικότερες ιδιότητες του συμβόλου $\binom{n}{k}$.

Πρόταση Γ΄.26. Υποθέτουμε ότι k και n είναι μη αρνητικοί ακέραιοι. Τότε ισχύουν τα ακόλουθα:

(i) Αν $k > n$, τότε $\binom{n}{k} = 0$.

(ii) $\binom{n}{n} = \binom{n}{0} = 1.$

(ii) $\binom{n}{1} = n.$

(iv) Αν $0 \leq k \leq n$, τότε $\binom{n}{k} = \dfrac{n!}{k!(n-k)!} = \binom{n}{n-k}$.

Απόδειξη: (i) Εφόσον $k > n \Leftrightarrow n - k < 0$ και ο $n-k$ είναι ακέραιος, θα έχουμε $n - k + 1 \leq 0$. Επομένως $n \geq 0 \geq n - k + 1$ και συνεπώς κάποιος από τους ακεραίους $n, n-1, \ldots, n-k+1$ πρέπει να είναι μηδέν. Άρα ο αριθμητής $n(n-1)\cdots(n-k+1)$ του $\binom{n}{k}$ είναι μηδέν.

(ii) Η σχέση $\binom{n}{0} = 1$ προκύπτει από τον ορισμό του συμβόλου $\binom{n}{k}$.

Τώρα, $\binom{n}{n} = \dfrac{n(n-1)(n-2)\cdots(n-n+1)}{n!} = \dfrac{n(n-1)(n-2)\cdots 1}{n!} = \dfrac{n!}{n!} = 1.$

(iii) $\binom{n}{1} = \dfrac{n}{1!} = n.$

(iv) Για $k = 0$ ή $k = n$ έχει αποδειχθεί προηγουμένως. Έστω $1 \leq k \leq n-1$. Τότε έχουμε: $\binom{n}{k} = \dfrac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \dfrac{n(n-1)(n-2)\cdots(n-k+1)(n-k)!}{n!(n-k)!} = \dfrac{n!}{n!(n-k)!}$. Από τον τύπο αυτό προκύπτει επίσης ότι $\binom{n}{n-k} = \dfrac{n!}{(n-k)!(n-(n-k))!} = \dfrac{n!}{(n-k)!k!} = \binom{n}{k}$. ■

Λήμμα Γ΄.27. (Ο τριγωνικός τύπος του Pascal) Αν $1 \leq k \leq n$, τότε ισχύει ο τύπος

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Απόδειξη: Αν $k = n$ τότε $\binom{n}{k} = \binom{n-1}{k-1} = 1$ και $\binom{n-1}{k} = 0$ και ο τύπος ισχύει σ΄ αυτή την περίπτωση.
Υποθέτουμε τώρα ότι $k < n \Leftrightarrow k \leq n-1$.
Έχουμε: $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n}{k} \cdot \frac{(n-1)!}{(k-1)!(n-k)!} = \frac{n}{k} \cdot \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} = \frac{n}{k} \cdot \binom{n-1}{k-1} =$
$= \frac{k+(n-k)}{k}\binom{n-1}{k-1} = \binom{n-1}{k-1} + \frac{n-k}{k}\binom{n-1}{k-1} = \binom{n-1}{k-1} + \frac{n-k}{k}\frac{(n-1)!}{(k-1)!(n-k)!} = \binom{n-1}{k-1} +$
$+ \frac{(n-1)!}{k!(n-k-1)!} = \binom{n-1}{k-1} + \binom{n-1}{k}.$ ■

Ο τύπος αυτός ορίζει τα σύμβολα $\binom{n}{k}$ κατά τρόπο «αναδρομικό». Με βάση λοιπόν τον τύπο του Pascal παίρνουμε το επόμενο τριγωνικό σχήμα, γνωστό ως **τρίγωνο του Pascal**:

$$\begin{array}{ccccccccccccc}
 & & & & & & \binom{0}{0}=1 & & & & & & \\
 & & & & & \swarrow & & \searrow & & & & & \\
 & & & & \binom{1}{0}=1 & & & & \binom{1}{1}=1 & & & & \\
 & & & \swarrow & & \searrow & & \swarrow & & \searrow & & & \\
 & & \binom{2}{0}=1 & & & \binom{2}{1}=2 & & & & \binom{2}{2}=1 & & & \\
 & \swarrow & & \searrow & \swarrow & & \searrow & \swarrow & & \searrow & & & \\
 \binom{3}{0}=1 & & & \binom{3}{1}=3 & & & \binom{3}{2}=3 & & & \binom{3}{3}=1 & & & \\
 \swarrow & & \searrow & \swarrow & & \searrow & \swarrow & & \searrow & \swarrow & & \searrow & \\
 \binom{4}{0}=1 & & & \binom{4}{1}=4 & & & \binom{4}{2}=6 & & & \binom{4}{3}=4 & & & \binom{4}{4}=1 \\
 \swarrow & & \searrow & \swarrow & & \searrow & \swarrow & & \searrow & \swarrow & & \searrow & \\
 \binom{5}{0}=1 & & & \binom{5}{1}=5 & & & \binom{5}{2}=10 & & & \binom{5}{3}=10 & & & \binom{5}{4}=5 \quad \binom{5}{5}=1 \\
 \swarrow & & \searrow & \swarrow & & \searrow & \swarrow & & \searrow & \swarrow & & \searrow & \\
 \binom{6}{0}=1 & & & \binom{6}{1}=6 & & & \binom{6}{2}=15 & & & \binom{6}{3}=20 & & & \binom{6}{4}=15 \quad \binom{6}{5}=6 \quad \binom{6}{6}=1
\end{array}$$

.....

Σχήμα 17: Τρίγωνο του Pascal

Στο τρίγωνο του Pascal κάθε αριθμός ισούται με το άθροισμα των δύο άλλων που βρίσκονται από πάνω, όπως δείχνουν τα βέλη.
Τώρα είμαστε σε θέση να διατυπώσουμε και να αποδείξουμε το βασικό θεώρημα αυτής της παραγράφου:

Θεώρημα Γ΄.28. (Το διώνυμο του Newton) Ισχύει η ακόλουθη αλγεβρική ταυτότητα:

$$(\alpha+\beta)^n = \sum_{k=0}^{n}\binom{n}{k}\alpha^{n-k}\beta^k \underset{\binom{n}{0}=\binom{n}{n}=1}{=} \alpha^n + \binom{n}{1}\alpha^{n-1}\beta + \binom{n}{2}\alpha^{n-2}\beta^2 + \binom{n}{3}\alpha^{n-3}\beta^3 + \cdots +$$
$$+ \binom{n}{n-3}\alpha^3\beta^{n-3} + \binom{n}{n-2}\alpha^2\beta^{n-2} + \binom{n}{n-1}\alpha\beta^{n-1} + \beta^n$$

.

Απόδειξη: Θα εφαρμόσουμε επαγωγή επί του n.
Για $n = 1$ έχουμε $(\alpha+\beta)^1 = \alpha+\beta = 1\cdot\alpha + 1\cdot\beta = \binom{1}{0}\alpha + \binom{1}{1}\beta$.
Άρα η πρόταση ισχύει για $n = 1$. (Θα μπορούσε κάποιος να ξεκινήσει την επαγωγή από το μηδέν θεωρώντας

την προφανή σχέση $(\alpha+\beta)^0 = 1 = \binom{0}{0}\alpha^0\beta^0$).
Υποθέτουμε ότι για κάποιο n ισχύει η σχέση

$$(\alpha+\beta)^n = \alpha^n + \binom{n}{1}\alpha^{n-1}\beta + \binom{n}{2}\alpha^{n-2}\beta^2 + \cdots + \binom{n}{n-2}\alpha^2\beta^{n-2} + \binom{n}{n-1}\alpha\beta^{n-1} + \beta^n. \quad \textbf{(1)}$$

Πολλαπλασιάζουμε τη σχέση (1) με α και παίρνουμε:

$$\alpha(\alpha+\beta)^n = \alpha^{n+1} + \binom{n}{1}\alpha^n\beta + \binom{n}{2}\alpha^{n-1}\beta^2 + \cdots + \binom{n}{n-2}\alpha^3\beta^{n-2} + \binom{n}{n-1}\alpha^2\beta^{n-1} + \alpha\beta^n. \quad \textbf{(2)}$$

Πολλαπλασιάζουμε τη σχέση (1) με β και παίρνουμε:

$$\beta(\alpha+\beta)^n = \alpha^n\beta + \binom{n}{1}\alpha^{n-1}\beta^2 + \binom{n}{2}\alpha^{n-2}\beta^3 + \cdots + \binom{n}{n-2}\alpha^2\beta^{n-1} + \binom{n}{n-1}\alpha\beta^n + \beta^{n+1}. \quad \textbf{(3)}$$

Αν προσθέσουμε τις (2) και (3) κατά μέλη, τότε στο αριστερό μέλος θα πάρουμε $(\alpha+\beta)(\alpha+\beta)^n = (\alpha+\beta)^{n+1}$. Στο δεξιό μέλος θα πάρουμε:

$$\alpha^{n+1} + \left(1+\binom{n}{1}\right)\alpha^n\beta + \left(\binom{n}{1}+\binom{n}{2}\right)\alpha^{n-1}\beta^2 + \left(\binom{n}{2}+\binom{n}{3}\right)\alpha^{n-2}\beta^3 + \cdots +$$
$$+ \left(\binom{n}{n-2}+\binom{n}{n-1}\right)\alpha^2\beta^{n-1} + \left(\binom{n}{n-1}+1\right)\alpha\beta^n + \beta^{n+1} =$$
$$= \alpha^{n+1} + \underbrace{\left(\binom{n}{0}+\binom{n}{1}\right)}_{\text{τρίγωνο Pascal}}\alpha^n\beta + \underbrace{\left(\binom{n}{1}+\binom{n}{2}\right)}_{\text{τρίγωνο Pascal}}\alpha^{n-1}\beta^2 + \underbrace{\left(\binom{n}{2}+\binom{n}{3}\right)}_{\text{τρίγωνο Pascal}}\alpha^{n-2}\beta^3 + \cdots +$$
$$+ \underbrace{\left(\binom{n}{n-2}+\binom{n}{n-1}\right)}_{\text{τρίγωνο Pascal}}\alpha^2\beta^{n-1} + \underbrace{\left(\binom{n}{n-1}+\binom{n}{n}\right)}_{\text{τρίγωνο Pascal}}\alpha\beta^n + \beta^{n+1} =$$
$$= \alpha^{n+1} + \binom{n+1}{1}\alpha^n\beta + \binom{n+1}{2}\alpha^{n-1}\beta^2 + \binom{n+1}{3}\alpha^{n-2}\beta^3 + \cdots \binom{n+1}{n-1}\alpha^2\beta^{n-1} + \binom{n+1}{n}\alpha\beta^n + \beta^{n+1}$$

και επειδή $\binom{n+1}{0} = \binom{n+1}{n+1} = 1$, έχουμε τελικώς

$$\binom{n+1}{0}\alpha^{n+1} + \binom{n+1}{1}\alpha^n\beta + \binom{n+1}{2}\alpha^{n-1}\beta^2 + \binom{n+1}{3}\alpha^{n-2}\beta^3 + \cdots \binom{n+1}{n-1}\alpha^2\beta^{n-1} + \binom{n+1}{n}\alpha\beta^n +$$
$$+ \binom{n+1}{n+1}\beta^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}\alpha^{n+1-k}\beta^k. \qquad \blacksquare$$

Επειδή $\binom{n}{k} = \binom{n}{n-k}$, το διώνυμο του Newton μπορεί να γραφεί και ως $(\alpha+\beta)^n = \sum_{k=0}^{n}\binom{n}{n-k}\alpha^{n-k}\beta^k$ ή καλύτερα, θεωρώντας ως βωβό δείκτη το $n-k \in \{0,1,\ldots,n\}$, οπότε το k θα αντικατασταθεί από το $n-k$, στη μορφή $(\alpha+\beta)^n = \sum_{k=0}^{n}\binom{n}{k}\alpha^k\beta^{n-k} = \beta^n + \binom{n}{1}\alpha\beta^{n-1} + \binom{n}{2}\alpha^2\beta^{n-2} + \cdots + \binom{n}{n-2}\alpha^{n-2}\beta^2 +$
$+ \binom{n}{n-1}\alpha^{n-1}\beta + \alpha^n.$

ΛΥΜΕΝΕΣ ΑΣΚΗΣΕΙΣ

Άσκηση 127. Να βρεθεί το ανάπτυγμα του $(\alpha+\beta)^{10}$.

Λύση: Έχουμε: $\binom{10}{1} = 10, \binom{10}{2} = \frac{10\cdot 9}{2} = 5\cdot 9 = 45, \binom{10}{3} = \frac{10\cdot 9\cdot 8}{6} = 10\cdot 3\cdot 4 = 120, \binom{10}{4} =$

$= \frac{10\cdot 9\cdot \cancel{8}\cdot 7}{\cancel{2}\cdot 3\cdot \cancel{4}} = 10\cdot 3\cdot 7 = 210$, $\binom{10}{5} = \frac{10\cdot 9\cdot 8\cdot 7\cdot 6}{2\cdot 3\cdot 4\cdot 5} = \frac{9\cdot 8\cdot 7\cdot 6}{3\cdot 4} = 3\cdot 2\cdot 7\cdot 6 = 36\cdot 7 = 252$. Οι υπόλοιποι διωνυμικοί συντελεστές είναι συμμετρικά ίσοι με αυτούς που μόλις βρήκαμε. Επομένως $(\alpha+\beta)^{10} = \alpha^{10}+10\alpha^9\beta+45\alpha^8\beta^2+120\alpha^7\beta^3+210\alpha^6\beta^4+252\alpha^5\beta^5+210\alpha^4\beta^6+120\alpha^3\beta^7+45\alpha^2\beta^8+10\alpha\beta^9+\beta^{10}$. ■

Άσκηση 128. Να αποδείξετε ότι:

(i) $\sum_{k=0}^{n}\binom{n}{k} = 2^n$.

(ii) $\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots = \binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots$.

(iii) $\sum_{k=1}^{n} k\binom{n}{k} = n\cdot 2^{n-1}$.

(iv) $\sum_{k=0}^{n}\frac{1}{k+1}\binom{n}{k} = \frac{2^{n+1}-1}{n+1}$.

Απόδειξη: (i) Στον τύπο του διωνύμου του Newton $\sum_{k=0}^{n}\binom{n}{k}\alpha^k\beta^{n-k}$ θέτουμε $\alpha=\beta=1$. Τότε $2^n = (1+1)^n = \binom{n}{0}1^0\cdot 1^n + \binom{n}{1}1^1\cdot 1^{n-1} + \binom{n}{2}1^2\cdot 1^{n-2} + \cdots + \binom{n}{n-1}1^{n-1}\cdot 1^1 + \binom{n}{n}1^n\cdot 1^0 = \binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n-1}+\binom{n}{n}$.

(ii) Στον τύπο του διωνύμου του Newton $\sum_{k=0}^{n}\binom{n}{k}\alpha^k\beta^{n-k}$ θέτουμε $\alpha=-1$ και $\beta=1$. Τότε $0 = 0^n = ((-1)+1)^n = \binom{n}{0}(-1)^0+\binom{n}{1}(-1)^1+\binom{n}{2}(-1)^2+\binom{n}{3}(-1)^3+\cdots+\binom{n}{n-1}(-1)^{n-1}+\binom{n}{n}(-1)^n = \binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\binom{n}{4}-\binom{n}{5}\cdots+\binom{n}{n-1}(-1)^{n-1}+\binom{n}{n}(-1)^n$, απ' όπου προκύπτει η αποδεικτέα.

(iii) 1ος τρόπος: Έχουμε: $1+\binom{n}{1}x+\binom{n}{2}x^2+\binom{n}{3}x^3+\cdots+\binom{n}{n-1}x^{n-1}+\binom{n}{n}x^n = (1+x)^n$. Αν παραγωγίσουμε, θα πάρουμε: $\binom{n}{1}+2\binom{n}{2}x+3\binom{n}{3}x^2+\cdots+(n-1)\binom{n}{n-1}x^{n-2}+n\binom{n}{n}x^{n-1} = n(1+x)^{n-1}$. Τέλος, θέτοντας $x=1$, παίρνουμε τη ζητούμενη σχέση.

2ος τρόπος: Για $k=1,2,\ldots,n$ έχουμε: $k\binom{n}{k} = k\cdot\frac{n!}{k!\cdot(n-k)!} = \frac{n\cdot(n-1)!}{(k-1)!\cdot((n-1)-(k-1))!} = n\cdot\binom{n-1}{k-1}$. Επομένως, $\sum_{k=1}^{n}k\binom{n}{k} = n\sum_{k=1}^{n}\binom{n-1}{k-1} \underset{k\text{ αντί }k-1}{=} n\sum_{k=0}^{n-1}\binom{n-1}{k} \underset{\text{σχέση (i)}}{=} n\cdot 2^{n-1}$.

(iv) 1ος τρόπος: Ολοκληρώνουμε στο $[0,1]$ τη σχέση $\sum_{k=0}^{n}\binom{n}{k}x^k = (1+x)^n$. Έχουμε: $\sum_{k=0}^{n}\binom{n}{k}\int_0^1 x^k dx = \int_0^1(1+x)^n dx \Leftrightarrow \sum_{k=0}^{n}\frac{1}{k+1}\binom{n}{k} = \frac{(1+x)^{n+1}}{n+1}\Big|_0^1 = \frac{2^{n+1}-1}{n+1}$.

2ος τρόπος: Για $k=0,1,2,\ldots,n$ έχουμε: $\frac{1}{k+1}\binom{n}{k} = \frac{1}{k+1}\cdot\frac{n!}{k!(n-k)!} = \frac{n!}{(k+1)!(n-k)!} = \frac{1}{n+1}\cdot\frac{(n+1)!}{(k+1)!((n+1)-(k+1))!} = \frac{1}{n+1}\binom{n+1}{k+1}$. Επομένως $\sum_{k=0}^{n}\frac{1}{k+1}\binom{n}{k} = \frac{1}{n+1}\sum_{k=0}^{n}\binom{n+1}{k+1} \underset{k\text{ αντί }k+1}{=} \frac{1}{n+1}\sum_{k=1}^{n+1}\binom{n+1}{k} = \frac{1}{n+1}\left(-1+\binom{n+1}{0}+\sum_{k=1}^{n+1}\binom{n+1}{k}\right) = \frac{1}{n+1}\left(\sum_{k=0}^{n+1}\binom{n+1}{k}-1\right) = \frac{1}{n+1}(2^{n+1}-1)$. ■

Άσκηση 129. Να αποδείξετε ότι:

(i) $\binom{n}{0}\binom{n}{n}+\binom{n}{1}\binom{n}{n-1}+\binom{n}{2}\binom{n}{n-2}+\binom{n}{3}\binom{n}{n-3}+\cdots+\binom{n}{n-1}\binom{n}{1}+\binom{n}{n}\binom{n}{0}=$
$=\binom{n}{0}^2+\binom{n}{1}^2+\binom{n}{2}^2+\binom{n}{3}^2+\cdots+\binom{n}{n-1}^2+\binom{n}{n}^2=\binom{2n}{n}$.
(ii) Γενικότερα, αν m, n είναι θετικοί ακέραιοι και $0\le r\le m+n$, να αποδείξετε την

(Ταυτότητα του Vandermonde) $$\sum_{i=0}^{r}\binom{m}{i}\binom{n}{r-i}=\binom{m+n}{r}.$$

Απόδειξη: (i) Εφόσον $\binom{n}{k}=\binom{n}{n-k}$, για κάθε $k=0,1,\ldots,n$, η πρώτη ισότητα προκύπτει άμεσα. Θεωρούμε τη σχέση $(1+x)^n(1+x)^n=(1+x)^{2n}$. Ο συντελεστής του x^n στο δεξιό μέλος της ισότητας αυτής είναι $\binom{2n}{n}$. Ο συντελεστής αυτός προκύπτει ως το άθροισμα των γινομένων των συντελεστών των x^i και x^{n-i} στα αναπτύγματα $(1+x)^n=\sum_{i=0}^{n}\binom{n}{i}$ των δύο παρενθέσεων στο αριστερό μέλος της ισότητας αυτής. Ο συντελεστής του x^i στο ανάπτυγμα της πρώτης παρένθεσης είναι $\binom{n}{i}$ και ο συντελεστής του x^{n-i} στο ανάπτυγμα της δεύτερης παρένθεσης είναι $\binom{n}{n-i}$. Το άθροισμά τους για τις διάφορες τιμές του i είναι $\sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i}$.

(ii) Αν γράψουμε $(1+x)^{m+n}=(1+x)^m(1+x)^n=\sum_{i=0}^{m}\binom{m}{i}x^i\cdot\sum_{j=0}^{n}\binom{n}{j}x^j$ και παρατηρήσουμε ότι ο συντελεστής του x^r στο αριστερό μέλος της ισότητας είναι $\binom{m+n}{r}$, ενώ στο δεξιό προκύπτει ως το άθροισμα των γινομένων $\binom{m}{i}\binom{n}{j}$ των συντελεστών x^i και x^j, όπου $i+j=r$, δηλαδή $j=r-i$, τότε προκύπτει το συμπέρασμα. ■

Κανονικά θα έπρεπε, αφ' ενός $0\le i\le r$ και $0\le i\le m$, οπότε $0\le i\le\min\{m,r\}$ και αφ' ετέρου $0\le j=r-i\le n\Leftrightarrow r-n\le i\le r$. Τελικώς $\max\{0,r-n\}\le i\le\min\{m,r\}$.Έτσι, πιο σωστά θα μπορούσαμε να γράψουμε $\sum_{i=\max\{0,\,r-n\}}^{\min\{r,\,m\}}\binom{m}{i}\binom{n}{r-i}=\binom{m+n}{r}$, αντί $\sum_{i=0}^{r}\binom{m}{i}\binom{n}{r-i}=\binom{m+n}{r}$. Αυτό βέβαια δεν επηρεάζει τον τύπο γιατί αν $i>m$ ή $r-i>n$, τότε οι αντίστοιχοι διωνυμικοί συντελεστές μηδενίζονται.

Παρατηρούμε ότι στην **άσκηση Γ΄.28** οι διωνυμικοί συντελεστές $1=\binom{10}{0}$, $10=\binom{10}{1}$, $45=\binom{10}{2}$, $120=\binom{10}{3}$, $210=\binom{10}{4}$, $252=\binom{10}{5}$ βαίνουν αυξανόμενοι, φτάνοντας τη μέγιστη τιμή $252=\binom{10}{5}$. Στη συνέχεια, συμμετρικά βαίνουν μειούμενοι. Αυτό δεν είναι τυχαίο. Η επόμενη άσκηση αναφέρεται στο φαινόμενο αυτό.

Άσκηση 130. Αν n θετικός ακέραιος, τότε: $\binom{n}{0}<\binom{n}{1}<\binom{n}{2}<\cdots\binom{n}{\lfloor\frac{n}{2}\rfloor}$.
Ειδικότερα, αν το $n=2r$ είναι άρτιος, τότε το πλήθος των όρων στο ανάπτυγμα του Newton είναι $n+1=$ $=2r+1$, περιττό και ο μεγαλύτερος διωνυμικός συντελεστής είναι ο μεσαίος $\binom{n}{\lfloor\frac{n}{2}\rfloor}=\binom{n}{\frac{n}{2}}=\binom{n}{r}$.
Αν το $n=2r+1$ είναι περιττός, τότε το πλήθος των όρων στο ανάπτυγμα του Newton είναι $n+1=2r+2$, άρτιο και υπάρχουν δύο μεσαίοι διωνυμικοί συντελεστές που είναι οι μεγαλύτεροι. Αυτοί είναι οι $\binom{n}{\lfloor\frac{n}{2}\rfloor}=$

$= \binom{n}{r}$ και $\binom{n}{r+1}$, γιατί $\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2r+1}{2} \right\rfloor = \left\lfloor r + \frac{1}{2} \right\rfloor = r$ και $\binom{n}{r} = \binom{2r+1}{r} = \binom{2r+1}{2r+1-r} =$
$= \binom{2r+1}{r+1} = \binom{n}{r+1}$.

Απόδειξη: Παρατηρούμε ότι αν $k \geq 1$, τότε $\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k)(n-k+1)}{k!} =$
$= \frac{n-k+1}{k} \cdot \frac{n(n-1)\cdots(n-k)}{(k-1)!} = \frac{n-k+1}{k}\binom{n}{k-1}$. Από αυτό προκύπτει ότι $\binom{n}{k} > \binom{n}{k-1} \Leftrightarrow$
$\Leftrightarrow n-k+1 > k \Leftrightarrow k < \frac{n+1}{2}$.

Αν $n = 2r$ άρτιος, τότε $k < \frac{n+1}{2} = \frac{2r+1}{2} = r + \frac{1}{2}$. Ο μεγαλύτερος ακέραιος που είναι μικρότερος του $r + \frac{1}{2}$ είναι ο $r = \frac{n}{2} = \left\lfloor \frac{n}{2} \right\rfloor$.

Αν $n = 2r+1$ περιττός, τότε $k < \frac{n+1}{2} = \frac{2r+2}{2} = r+1$. Ο μεγαλύτερος ακέραιος που είναι μικρότερος του $r+1$ είναι πάλι ο r. Αλλά τότε, $\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor r + \frac{1}{2} \right\rfloor = r$. ■

Γ΄.3 Η επαγωγή και οι άλλες αποδεικτικές μέθοδοι

Από τα παραπάνω καθίσταται σαφές ότι η επαγωγή αποτελεί ισχυρό αποδεικτικό εργαλείο. Συνήθως όμως οι αποδείξεις που βασίζονται στην επαγωγή δεν διακρίνονται για την κομψότητά τους. Επίσης, κατά την επαγωγική διαδικασία θα πρέπει να μαντέψει κάποιος έναν τύπο, μια σχέση κτλ, δοκιμάζοντας για μικρές σχετικά τιμές του n, κάτι το οποίο δεν είναι πάντοτε εύκολη υπόθεση. Με άλλα λόγια, η επαγωγή δεν αποτελεί πάντα ισχυρό **ευρετικό** εργαλείο. Ας δούμε την επόμενη άσκηση:

Άσκηση 131. Να υπολογίσετε τα αθροίσματα
(i) $S_1 = 1 + 2 + \cdots + n$ και
(ii) $S_2 = 1^2 + 2^2 + \cdots + n^2$.
(iii) Αν $S_k = 1^k + 2^k + 3^k + \cdots + n^k$, τότε να αποδείξετε την αναδρομική σχέση

$$S_{k+1} = \frac{1}{k+2}\left((n+1)\left((n+1)^{k+1} - 1\right) - \binom{k+2}{2}S_k - \binom{k+2}{3}S_{k-1} - \cdots \binom{k+2}{k}S_2 - \binom{k+2}{k+1}S_1\right)$$

Απόδειξη: (i) 1ος τρόπος: Έστω $S_1 = 1+2+\cdots+n$. Γράφοντας ανάποδα τους προσθεταίους παίρνουμε τις ακόλουθες δύο σχέσεις:

$$\begin{array}{lccccccccccc} S_1 & = 1 & + & 2 & + & 3 & + & \cdots & + & (n-3) & + & (n-1) & + & n \\ S_1 & = n & + & (n-1) & + & (n-2) & + & \cdots & + & 3 & + & 2 & + & 1 \end{array}$$

Αν προσθέσουμε κατά μέλη και κατά στήλες, θα πάρουμε στο δεύτερο μέλος n αθροίσματα $n+1$, $n-1+2 = n+1$, $n-2+3 = n+1$, δηλαδή όλα ίσα με $n+1$. Άρα το δεύτερο μέλος της σχέσης που θα προκύψει ισούται με $n(n+1)$. Το πρώτο φυσικά ισούται με $2S_1$, οπότε $2S_1 = n(n+1) \Leftrightarrow S_1 = \frac{n(n+1)}{2}$.

2ος τρόπος: Χρησιμοποιούμε την ταυτότητα $(k+1)^2 = k^2 + 2k + 1$. Έχουμε (με πρόσθεση κατά μέλη και διαγραφή εκατέρωθεν):

$$\begin{array}{rcccccc} \cancel{2^2} & = & 1^2 & + & 2\cdot & 1 & +1 \\ \cancel{3^2} & = & \cancel{2^2} & + & 2\cdot & 2 & +1 \\ \cancel{4^2} & = & \cancel{3^2} & + & 2\cdot & 3 & +1 \\ & \vdots & & & & & \\ \cancel{(n-2)^2} & = & \cancel{(n-3)^2} & + & 2\cdot & (n-3) & +1 \\ \cancel{(n-1)^2} & = & \cancel{(n-2)^2} & + & 2\cdot & (n-2) & +1 \\ \cancel{n^2} & = & \cancel{(n-1)^2} & + & 2\cdot & (n-1) & +1 \\ (n+1)^2 & = & \cancel{n^2} & + & 2\cdot & n & +1 \end{array}$$

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

δηλαδή $(n+1)^2 = 1+2\mathrm{S}_1+n \Leftrightarrow 2\mathrm{S}_1 = (n+1)^2-(n+1) = (n+1)(n+1-1) = n(n+1)$. Άρα $\mathrm{S}_1 = \dfrac{n(n+1)}{2}$.

3ος τρόπος: Σε μια συγκέντρωση παρευρέθηκαν $n+1$ άτομα. Πόσες χειραψίες ανταλλάχτηκαν;
Κάθε ένας από τους $n+1$ παρευρισκόμενους ανταλλάζει n χειραψίες με τους υπόλοιπους n. Σύνολο λοιπόν $(n+1)n$ χειραψίες. Αλλά όμως, σ᾽ αυτή τη μέτρηση κάθε χειραψία μετριέται δύο φορές. Π.χ. Όταν ο Α και Β χαιρετιούνται, η χειραψία αυτή μετριέται και όταν υπολογίζουμε τις χειραψίες του Α, αλλά και όταν υπολογίζουμε τις χειραψίες του Β. Ο σωστός αριθμός των χειραψιών είναι λοιπόν $\dfrac{n(n+1)}{2}$.
Μπορούμε να μετρήσουμε τις χειραψίες και διαφορετικά: Στην αρχή έρχεται ο πρώτος και δεν βρίσκει κανέναν. Μετά έρχεται ο δεύτερος και χαιρετά τον πρώτο: 1 χειραψία. Μετά έρχεται ο τρίτος και χαιρετά τους δύο πρώτους: άλλες 2 χειραψίες. Μετά έρχεται ο τέταρτος και χαιρετά τους τρεις πρώτους: άλλες 3 χειραψίες. κ.ο.κ. Τελικά θα έρθει και ο τελευταίος, ο $(n+1)-$στος και θα χαιρετήσει τους n που έχουν ήδη έρθει. Σύνολο χειραψιών: $1+2+3+\cdots+n$. Άρα $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$.

Σημείωση: Η τελευταία μέθοδος μπορεί να εφαρμοστεί και στην άσκηση Γ΄.12. Από κάθε κορυφή ξεκινούν $n-3$ διαγώνιοι. Σύνολο διαγωνίων $n(n-3)$. Αλλά κατ᾽ αυτή την μέτρηση κάθε διαγώνιος μετριέται δύο φορές. Για παράδειγμα, η διαγώνιος A_1A_3 μετριέται και όταν υπολογίζουμε τις διαγωνίους που ξεκινούν από το A_1, αλλά και όταν υπολογίζουμε τις διαγωνίους που ξεκινούν από το A_3. Άρα το σωστό πλήθος είναι $\dfrac{n(n-3)}{2}$. Η απόδειξη αυτή είναι προφανώς απλούστερη από την επαγωγική απόδειξη.

(ii) Για το S_2 θα χρησιμοποιήσουμε τον δεύτερο τρόπο του προηγουμένου ζητήματος. Εδώ θα χρησιμοποιήσουμε την ταυτότητα $(k+1)^3 = k^3+3k^2+3k+1$ και θα θεωρήσουμε δεδομένο τον τύπο για το S_1. Έχουμε τις σχέσεις:

$$\begin{array}{rcccccccccc}
\cancel{2^3} &=& 1^3 &+& 3\cdot & 1^2 &+& 3\cdot 1 &+& 1\\
\cancel{3^3} &=& \cancel{2^3} &+& 3\cdot & 2^2 &+& 3\cdot 2 &+& 1\\
\cancel{4^3} &=& \cancel{3^3} &+& 3\cdot & 3^2 &+& 3\cdot 3 &+& 1\\
 & & \vdots & & & & & & & \\
\cancel{(n-1)^3} &=& \cancel{(n-2)^3} &+& 2\cdot & (n-2)^2 &+& 3\cdot(n-2) &+& 1\\
\cancel{n^3} &=& \cancel{(n-1)^3} &+& 3\cdot & (n-1)^2 &+& 3\cdot(n-1) &+& 1\\
(n+1)^3 &=& \cancel{n^3} &+& 3\cdot & n^2 &+& 3\cdot n &+& 1
\end{array}$$

$$(n+1)^3 = 1+3\cdot\mathrm{S}_2+3\cdot\mathrm{S}_1+n,$$

δηλαδή $3\mathrm{S}_2 = (n+1)^3-(n+1)-3\mathrm{S}_1 = (n+1)^3-(n+1)-3\cdot\dfrac{n(n+1)}{2} = (n+1)\left((n+1)^2-1-\dfrac{3n}{2}\right) =$
$= (n+1)\dfrac{2n^2+4n+2-2-3n}{2} = \dfrac{(n+1)(2n^2+n)}{2} = \dfrac{n(n+1)(2n+1)}{2}$. Άρα $\mathrm{S}_2 = \dfrac{n(n+1)(2n+1)}{6}$.

(iii) Χρησιμοποιούμε τον τύπο του διωνύμου του Newton σε συνδυασμό με την προηγούμενη μέθοδο. Έχουμε:

$$\begin{array}{rcccccccc}
\cancel{2^{k+2}} &=& 1^{k+2} &+& \binom{k+2}{1}\cdot 1^{k+1} &+& \binom{k+2}{2}\cdot 1^{k} &+& \binom{k+2}{3}\cdot 1^{k-1} &+\cdots+& \binom{k+2}{k+1}1^1+1\\
\cancel{3^{k+2}} &=& \cancel{2^{k+2}} &+& \binom{k+2}{1}\cdot 2^{k+1} &+& \binom{k+2}{2}\cdot 2^{k} &+& \binom{k+2}{3}\cdot 2^{k-1} &+\cdots+& \binom{k+2}{k+1}2^1+1\\
\cancel{4^{k+2}} &=& \cancel{3^{k+2}} &+& \binom{k+2}{1}\cdot 3^{k+1} &+& \binom{k+2}{2}\cdot 3^{k} &+& \binom{k+2}{3}\cdot 3^{k-1} &+\cdots+& \binom{k+2}{k+1}3^1+1\\
 & & \vdots & & & & & & & & \\
\cancel{(n-1)^{k+2}} &=& \cancel{(n-2)^{k+2}} &+& \binom{k+2}{1}\cdot (n-2)^{k+1} &+& \binom{k+2}{2}\cdot (n-2)^{k} &+& \binom{k+2}{3}\cdot (n-2)^{k-1} &+\cdots+& \binom{k+2}{k+1}(n-2)^1+1\\
\cancel{n^{k+2}} &=& \cancel{(n-1)^{k+2}} &+& \binom{k+2}{1}\cdot (n-1)^{k+1} &+& \binom{k+2}{2}\cdot (n-1)^{k} &+& \binom{k+2}{3}\cdot (n-1)^{k-1} &+\cdots+& \binom{k+2}{k+1}(n-1)^1+1\\
(n+1)^{k+2} &=& \cancel{n^{k+2}} &+& \binom{k+2}{1}\cdot n^{k+1} &+& \binom{k+2}{2}\cdot n^{k} &+& \binom{k+2}{3}\cdot n^{k-1} &+\cdots+& \binom{k+2}{k+1}n^1+1
\end{array}$$

Προσθέτοντας κατά μέλη και διαγράφοντας εκατέρωθεν τους ίσους όρους παίρνουμε:

$$(n+1)^{k+2} = 1+\binom{k+2}{1}\mathrm{S}_{k+1}+\binom{k+2}{2}\mathrm{S}_k+\binom{k+2}{3}\mathrm{S}_{k-1}+\cdots\binom{k+2}{k+1}\mathrm{S}_1+n,$$

απ᾽ όπου προκύπτει η αναγωγική σχέση. ■

Στην **άσκηση Γ΄.6 γ)** αποδείξαμε με επαγωγή ότι $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n(n+1)}=\sum_{k=1}^{n}\frac{1}{k(k+1)}=\frac{n}{n+1}$. Αν όμως παρατηρήσουμε ότι $\frac{1}{k(k+1)}=\frac{1}{k}-\frac{1}{k+1}$. (Αυτό θυμίζει την τεχνική διάσπασης κλασμάτων κατά τον υπολογισμό ολοκληρωμάτων), τότε θα πάρουμε $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{\not 2}+\frac{1}{\not 2}-\frac{1}{\not 3}+\frac{1}{\not 3}-\frac{1}{\not 4}+\cdots+\frac{1}{\not n}-\frac{1}{n+1}==1-\frac{1}{n+1}=\frac{n}{n+1}$.
Βλέπουμε λοιπόν ότι με τη μέθοδο αυτή υπολογίζουμε κατευθείαν το αποτέλεσμα, χωρίς προηγουμένως να το μαντέψουμε και στη συνέχεια να το επαληθεύσουμε με επαγωγή.
Στην άσκηση Γ΄.10 αποδείξαμε με επαγωγή ότι $\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots+\frac{n}{2^n}=2-\frac{n+2}{2^n}$. Μπορούμε, χωρίς να καταφύγουμε στην επαγωγή να υπολογίσουμε κάτι γενικότερο.
Έστω το άθροισμα $\mathrm{S}=\alpha+2\alpha^2+3\alpha^3+\cdots+(n-1)\alpha^{n-1}+n\alpha^n$, όπου $\alpha\neq 1$. Τότε $\alpha\mathrm{S}=\alpha^2+2\alpha^3+3\alpha^4+\cdots+(n-1)\alpha^n+n\alpha^{n+1}$. Επομένως $(1-\alpha)\mathrm{S}=\alpha+\alpha^2+\alpha^3+\cdots+\alpha^n-n\alpha^{n+1}=\alpha(1+\alpha+\alpha^2+\cdots+\alpha^{n-1})-n\alpha^{n+1}=\alpha\cdot\frac{1-\alpha^n}{1-\alpha}-n\alpha^{n+1}$. Άρα $(1-\alpha)\mathrm{S}=\frac{\alpha-\alpha^{n+1}-n\alpha^{n+1}+n\alpha^{n+2}}{1-\alpha}=\frac{\alpha-(n+1)\alpha^{n+1}+n\alpha^{n+2}}{1-\alpha}\Rightarrow \mathrm{S}=\frac{\alpha-(n+1)\alpha^{n+1}+n\alpha^{n+2}}{(1-\alpha)^2}$. Αν θέσουμε $\alpha=\frac{1}{2}$, τότε θα πάρουμε $\mathrm{S}=\frac{\frac{1}{2}-(n+1)\left(\frac{1}{2}\right)^{n+1}+n\left(\frac{1}{2}\right)^{n+2}}{\left(1-\frac{1}{2}\right)^2}=4\left(\frac{1}{2}-(n+1)\left(\frac{1}{2}\right)^{n+1}+n\left(\frac{1}{2}\right)^{n+2}\right)=2-(n+1)\left(\frac{1}{2}\right)^{n-1}+n\left(\frac{1}{2}\right)^n=2-(2n+2-n)\left(\frac{1}{2}\right)^n=2-\frac{n+2}{2^n}$.

Θα δώσουμε στη συνέχεια δύο άλλες αποδείξεις (χωρίς επαγωγή) της ανισότητας Cauchy:

$$\left(\sum_{i=1}^{n}\alpha_i^2\right)\cdot\left(\sum_{i=1}^{n}\beta_i^2\right)\geq\left(\sum_{i=1}^{n}\alpha_i\beta_i\right)^2.$$

Λήμμα Γ΄.29. (Ταυτότητα Lagrange) Ισχύει η σχέση:

$$\left(\sum_{i=1}^{n}\alpha_i^2\right)\cdot\left(\sum_{i=1}^{n}\beta_i^2\right)-\left(\sum_{i=1}^{n}\alpha_i\beta_i\right)^2=\sum_{1\leq i<j\leq n}\begin{vmatrix}\alpha_i & \beta_i\\ \alpha_j & \beta_j\end{vmatrix}^2.$$

Απόδειξη: Το γινόμενο $(\alpha_1^2+\alpha_2^2+\alpha_3^2+\cdots+\alpha_n^2)(\beta_1^2+\beta_2^2+\beta_3^2+\cdots+\beta_n^2)$ θα μας δώσει το άθροισμα $\alpha_1^2\beta_1^2+\alpha_2^2\beta_2^2+\alpha_3^2\beta_3^2+\cdots+\alpha_n^2\beta_n^2$, όρους δηλαδή με τον ίδιο δείκτη για τα α_i και β_i συν όλους τους όρους της μορφής $\alpha_i^2\beta_j^2$, όπου $i\neq j$. Για κάθε τέτοιο όρο $\alpha_i^2\beta_j^2$, με $i\neq j$ θεωρούμε τον αντίστοιχο τον $\alpha_j^2\beta_i^2$ και στο τελικό άθροισμα τους προσθέτουμε σε ζεύγη της μορφής $\alpha_i^2\beta_j^2+\alpha_j^2\beta_i^2$. Επειδή η παράσταση $\alpha_i^2\beta_j^2+\alpha_j^2\beta_i^2$ είναι συμμετρική ως προς τους δείκτες i,j, δεν παίζει ρόλο ποιος είναι ο μεγαλύτερος και ποιος ο μικρότερος. Είτε είναι ο i είτε είναι ο j, η τιμή της παράστασης $\alpha_i^2\beta_j^2+\alpha_j^2\beta_i^2$ είναι ίδια. Συνοψίζοντας τα προηγούμενα, έχουμε:

$$(\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2)(\beta_1^2+\beta_2^2+\cdots+\beta_n^2)=\alpha_1^2\beta_1^2+\alpha_2^2\beta_2^2+\cdots+\alpha_n^2\beta_n^2+\sum_{1\leq i<j\leq n}(\alpha_i^2\beta_j^2+\alpha_j^2\beta_i^2).\quad\textbf{(1)}$$

Τώρα, το τετράγωνο $(\alpha_1\beta_1+\alpha_2\beta_2+\alpha_3\beta_3+\cdots+\alpha_n\beta_n)^2$ θα μας δώσει πάλι το άθροισμα $\alpha_1^2\beta_1^2+\alpha_2^2\beta_2^2+\alpha_3^2\beta_3^2+\cdots+\alpha_n^2\beta_n^2$ συν όρους της μορφής $\alpha_i\beta_i\alpha_j\beta_j=\alpha_i\beta_j\alpha_j\beta_i$, όπου $i\neq j$. Οι τελευταίοι αυτοί όροι εμφανίζονται δύο φορές στο τελικό άθροισμα. Πράγματι, επειδή $(\alpha_1\beta_1+\alpha_2\beta_2+\alpha_3\beta_3+\cdots+\alpha_n\beta_n)^2==(\alpha_1\beta_1+\alpha_2\beta_2+\alpha_3\beta_3+\cdots+\alpha_n\beta_n)(\alpha_1\beta_1+\alpha_2\beta_2+\alpha_3\beta_3+\cdots+\alpha_n\beta_n)$, ο όρος πχ. $\alpha_2\beta_2\alpha_3\beta_3$ θα εμφανιστεί αν πάρουμε το $\alpha_2\beta_2$ από την πρώτη παρένθεση και το $\alpha_3\beta_3$ από τη δεύτερη ή το ανάποδο, αν δηλαδή πάρουμε το $\alpha_3\beta_3$ από την πρώτη παρένθεση και το $\alpha_2\beta_2$ από τη δεύτερη. Άρα ο όρος αυτό θα έχει συντελεστή 2 στο τελικό άθροισμα. Γενικά ο όρος $\alpha_i\beta_i\alpha_j\beta_j$ θα έχει συντελεστή 2. Επειδή $i\neq j$ κάποιος από τους δείκτες

αυτούς είναι ο μικρότερος και ο άλλος ο μεγαλύτερος. Επειδή και οι δύο δείκτες εμφανίζονται συμμετρικά στο γινόμενο $\alpha_i\beta_i\alpha_j\beta_j$, δεν παίζει ρόλο ποιο σύμβολο θα επιλέξουμε για το μικρότερο και ποιο για το μεγαλύτερο. Από τα προηγούμενα προκύπτει λοιπόν ότι

$$(\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n)^2=\alpha_1^2\beta_1^2+\alpha_2^2\beta_2^2+\cdots+\alpha_n^2\beta_n^2+2\sum_{1\le i<j\le n}\alpha_i\beta_j\alpha_j\beta_i. \quad \textbf{(2)}$$

Αν αφαιρέσουμε κατά μέλη τις σχέσεις (1) και (2), θα πάρουμε:
$(\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2)(\beta_1^2+\beta_2^2+\cdots+\beta_n^2)-(\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n)^2=\sum_{1\le i<j\le n}(\alpha_i^2\beta_j^2+\alpha_j^2\beta_i^2-2\alpha_i\beta_j\alpha_j\beta_i)=$

$$=\sum_{1\le i<j\le n}(\alpha_i\beta_j-\alpha_j\beta_i)^2=\sum_{1\le i<j\le n}\begin{vmatrix}\alpha_i & \beta_i\\ \alpha_j & \beta_j\end{vmatrix}^2.$$ ■

2η Απόδειξη της ανισότητας Cauchy: Επειδή το δεύτερο μέρος της ταυτότητας Lagrange είναι άθροισμα τετραγώνων, το πρώτο μέλος είναι μη αρνητικό, οπότε προκύπτει η ανισότητα Cauchy. ■

Επίσης, για να ισχύει ως ισότητα η ανισότητα Cauchy, θα πρέπει όλες οι ορίζουσες στο δεύτερο μέλος της ταυτότητας Lagrange να είναι μηδέν. Σ' αυτή την περίπτωση, αν κάποιο από τα διανύσματα $(\alpha_1,\alpha_2,\ldots,\alpha_n)$, $(\beta_1,\beta_2,\ldots,\beta_n)$ δεν είναι μηδενικό, πχ. το $(\alpha_1,\alpha_2,\ldots,\alpha_n)$, τότε το άλλο είναι πολλαπλάσιο αυτού. Αν $(\alpha_1,\alpha_2,\ldots,\alpha_n)\neq\mathbf{0}$, δηλαδή $\alpha_k\neq 0$, για κάποιο k, τότε θέτουμε $\lambda=\dfrac{\beta_k}{\alpha_k}\Leftrightarrow\beta_k=\lambda\alpha_k$. Τότε, επειδή για κάθε $i\neq k$, θα έχουμε $\begin{vmatrix}\alpha_i & \beta_i\\ \alpha_k & \beta_k\end{vmatrix}=0\Leftrightarrow\alpha_k\beta_i=\alpha_i\beta_k\Leftrightarrow\beta_i=\dfrac{\beta_k}{\alpha_k}\cdot\alpha_i=\lambda\alpha_i$.
Επομένως $(\beta_1,\beta_2,\ldots,\beta_n)=\lambda\cdot(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

3η Απόδειξη της ανισότητας Cauchy: Για κάθε $i=1,2,\ldots,n$ έχουμε $(\alpha_i x-\beta_i)^2=$
$=\alpha_i^2x^2-2\alpha_i\beta_i x+\beta_i^2\ge 0$, για κάθε $x\in\mathbb{R}$. Αν αθροίσουμε όλες αυτές τις σχέσεις θα πάρουμε:

$$\left(\sum_{i=1}^n\alpha_i^2\right)x^2-2\left(\sum_{i=1}^n\alpha_i\beta_i\right)x+\sum_{i=1}^n\beta_i^2\ge 0,\text{ για κάθε } x\in\mathbb{R}.$$

Αν $(\alpha_1,\alpha_2,\ldots,\alpha_n)=\mathbf{0}$, δηλαδή $\alpha_1=\alpha_2=\cdots=\alpha_n=0$, τότε η ανισότητα Cauchy ισχύει ως ισότητα. $(0=0)$. Και φυσικά σ' αυτή την περίπτωση $(\alpha_1,\alpha_2,\ldots,\alpha_n)=0\cdot(\beta_1,\beta_2,\ldots,\beta_n)$.
Έστω ότι κάποιος α_i δεν είναι μηδέν. Τότε $\mathrm{A}=\sum_{i=1}^n\alpha_i^2>0$. Αν $\mathrm{B}=\sum_{i=1}^n\beta_i^2$ και $\Gamma=\sum_{i=1}^n\alpha_i\beta_i$, τότε επειδή το τριώνυμο $\mathrm{A}x^2-2\Gamma x+\mathrm{B}$ είναι μη αρνητικό, για κάθε $x\in\mathbb{R}$, η διακρίνουσά του $\Delta=4\Gamma^2-4\mathrm{A}\cdot\mathrm{B}\le 0$. Δηλαδή $\mathrm{A}\cdot\mathrm{B}\ge\Gamma^2$ και τελειώσαμε. ■

Αν η ανισότητα Cauchy ισχύει ως ισότητα, δηλαδή η διακρίνουσα του τριωνύμου $\mathrm{A}x^2-2\Gamma x+\mathrm{B}$ είναι μηδέν, τότε η (αναγκαστικά) διπλή ρίζα $\lambda=\dfrac{\Gamma}{\mathrm{A}}$ θα πρέπει να μηδενίζει όλα τα τετράγωνα $(\alpha_i x-\beta_i)^2$. (Γιατί το τριώνυμο είναι το άθροισμά τους). Άρα $\beta_i=\lambda\alpha_i$, για κάθε $i=1,2,\ldots,n$, ήτοι $(\beta_1,\beta_2,\ldots,\beta_n)=\lambda\cdot(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

Στη συνέχεια θα δούμε πώς με μεθόδους **Γραμμικής Άλγεβρας** καταλήγουμε στον μάλλον περίεργο τύπο για τους αριθμούς Fibonacci.

Θεωρούμε το διάνυσμα-στήλη $\mathrm{P}_n=\begin{pmatrix}f_{n+1}\\ f_n\end{pmatrix}$. Προφανώς $\mathrm{P}_1=\begin{pmatrix}1\\ 1\end{pmatrix}$. Οι σχέσεις $\begin{cases}f_{n+2} &= f_{n+1}+f_n\\ f_{n+1} &= f_{n+1}\end{cases}$ γράφονται σε πινακική μορφή ως εξής: $\mathrm{P}_{n+1}=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}f_{n+1}\\ f_n\end{pmatrix}=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\mathrm{P}_n$. Επομένως $\mathrm{P}_n=$
$=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\mathrm{P}_{n-1}=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}^2\mathrm{P}_{n-2}=\cdots=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}^{n-1}\mathrm{P}_1$.
Για να υπολογίσουμε τη δύναμη του πίνακα $\mathrm{A}=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$ τον διαγωνοποιούμε. Το χαρακτηριστικό του

πολυώνυμο είναι $\phi(x)=\begin{vmatrix} x-1 & -1 \\ -1 & x \end{vmatrix}=x^2-x-1$, με ρίζες $\rho=\dfrac{1+\sqrt{5}}{2}$ και $\sigma=\dfrac{1-\sqrt{5}}{2}$.

Υπολογίζουμε τα αντίστοιχα ιδιοδιανύσματα: $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} \rho x \\ \rho y \end{pmatrix}\Leftrightarrow\begin{cases} x+y &= \rho x \\ x &= \rho y \end{cases}\Leftrightarrow$

$\Leftrightarrow\begin{cases} (\rho+1)y &= \rho^2 y \\ x &= \rho y \end{cases}\Leftrightarrow\begin{cases} (\rho^2-\rho-1)y &= 0 \\ x &= \rho y \end{cases}\Leftrightarrow\begin{cases} 0 &= 0 \\ x &= \rho y \end{cases}\Leftrightarrow x=\rho y$. Για $y=1$ παίρνουμε το ιδιοδιάνυσμα $\begin{pmatrix} \rho \\ 1 \end{pmatrix}$. Ομοίως, το $\begin{pmatrix} \sigma \\ 1 \end{pmatrix}$ είναι ένα ιδιοδιάνυσμα του A που αντιστοιχεί στην ιδιοτιμή σ.

Έστω $\mathfrak{Q}=\begin{pmatrix} \rho & \sigma \\ 1 & 1 \end{pmatrix}$. Τότε $\mathrm{A}=\mathfrak{Q}\begin{pmatrix} \rho & 0 \\ 0 & \sigma \end{pmatrix}\mathfrak{Q}^{-1}$ και επομένως $\mathrm{A}^k=\mathfrak{Q}\begin{pmatrix} \rho^k & 0 \\ 0 & \sigma^k \end{pmatrix}\mathfrak{Q}^{-1}$, για κάθε φυσικό αριθμό k. Επίσης, $\det\mathfrak{Q}=\rho-\sigma=\sqrt{5}$ και $\mathrm{adj}\mathfrak{Q}=\begin{pmatrix} 1 & -\sigma \\ -1 & \rho \end{pmatrix}$ και άρα $\mathfrak{Q}^{-1}=\dfrac{1}{\sqrt{5}}\begin{pmatrix} 1 & -\sigma \\ -1 & \rho \end{pmatrix}$.

Επομένως

$$\mathrm{P}_n=\frac{1}{\sqrt{5}}\begin{pmatrix} \rho & \sigma \\ 1 & 1 \end{pmatrix}\begin{pmatrix} \rho^{n-1} & 0 \\ 0 & \sigma^{n-1} \end{pmatrix}\begin{pmatrix} 1 & -\sigma \\ -1 & \rho \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}=$$
$$=\frac{1}{\sqrt{5}}\begin{pmatrix} \rho^n-\sigma^n & \rho\sigma^n-\sigma\rho^n \\ \rho^{n-1}-\sigma^{n-1} & \rho\sigma^{n-1}-\sigma\rho^{n-1} \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}=\frac{1}{\sqrt{5}}\begin{pmatrix} \rho^n-\sigma^n+\rho\sigma^n-\sigma\rho^n \\ \rho^{n-1}-\sigma^{n-1}+\rho\sigma^{n-1}-\sigma\rho^{n-1} \end{pmatrix}=$$
$$=\frac{1}{\sqrt{5}}\begin{pmatrix} \rho^n(1-\sigma)-\sigma^n(1-\rho) \\ \rho^{n-1}(1-\sigma)-\sigma^{n-1}(1-\rho) \end{pmatrix}.$$

Αλλά $1-\sigma=\rho\Leftrightarrow 1-\rho=\sigma$. Επομένως $\mathrm{P}_n=\begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix}=\dfrac{1}{\sqrt{5}}\begin{pmatrix} \rho^{n+1}-\sigma^{n+1} \\ \rho^n-\sigma^n \end{pmatrix}$.

Κατά συνέπεια $f_n=\dfrac{1}{\sqrt{5}}\left(\rho^n-\sigma^n\right)=\dfrac{1}{\sqrt{5}}\left(\left(\dfrac{1+\sqrt{5}}{2}\right)^n-\left(\dfrac{1-\sqrt{5}}{2}\right)^n\right)$.

Τελειώνοντας την «κριτική» της επαγωγής ως ευρετικού εργαλείου, ας δούμε ένα άλλο παράδειγμα:

Άσκηση 132. Δίνεται η ακολουθία (α_n), με $\alpha_1=2$ και $\alpha_{n+1}=\frac{2}{3}\alpha_n+5$. Να βρεθεί το $\lim\limits_{n\to+\infty}\alpha_n$.

Λύση: Κατ' αρχάς δεν ξέρουμε αν η ακολουθία (α_n) συγκλίνει. Θα προσπαθήσουμε να βρούμε τον γενικό τύπο της ακολουθίας αυτής. Θα τον βρούμε κατευθείαν, χωρίς να τον «μαντέψουμε» και μετά να τον επαληθεύσουμε με επαγωγή. Γράφουμε σε στήλη την αναδρομική σχέση $\alpha_{n+1}=\frac{2}{3}\alpha_n+5$ για τις διάφορες τιμές του n.

$$\left.\begin{array}{ll} \alpha_1=2 & (1) \\ \alpha_2=\frac{2}{3}\alpha_1+5 & (2) \\ \alpha_3=\frac{2}{3}\alpha_2+5 & (3) \\ \vdots & \\ \alpha_{n-2}=\frac{2}{3}\alpha_{n-3}+5 & (n-2) \\ \alpha_{n-1}=\frac{2}{3}\alpha_{n-2}+5 & (n-1) \\ \alpha_n=\frac{2}{3}\alpha_{n-1}+5 & (n) \end{array}\right\}$$

Αν πολλαπλασιάσουμε τη $(n-1)$-στή σχέση με $\frac{2}{3}$, την $(n-2)$-στή σχέση με $\left(\frac{2}{3}\right)^2$ κ.ο.κ. έως την πρώτη σχέση με $\left(\frac{2}{3}\right)^{n-1}$, θα πάρουμε τις σχέσεις:

$$\left.\begin{array}{rcll} \cancel{\left(\frac{2}{3}\right)^{n-1}\alpha_1} &=& 2\left(\frac{2}{3}\right)^{n-1} & (1)' \\ \cancel{\left(\frac{2}{3}\right)^{n-2}\alpha_2} &=& \cancel{\left(\frac{2}{3}\right)^{n-1}\alpha_1}+5\cdot\left(\frac{2}{3}\right)^{n-2} & (2)' \\ \cancel{\left(\frac{2}{3}\right)^{n-3}\alpha_3} &=& \cancel{\left(\frac{2}{3}\right)^{n-2}\alpha_2}+5\cdot\left(\frac{2}{3}\right)^{n-3} & (3)' \\ & \vdots & & \\ \cancel{\left(\frac{2}{3}\right)^{2}\alpha_{n-2}} &=& \cancel{\left(\frac{2}{3}\right)^{3}\alpha_{n-3}}+5\cdot\left(\frac{2}{3}\right)^{2} & (n-2)' \\ \cancel{\frac{2}{3}\alpha_{n-1}} &=& \cancel{\left(\frac{2}{3}\right)^{2}\alpha_{n-2}}+5\cdot\frac{2}{3} & (n-1)' \\ \alpha_n &=& \cancel{\frac{2}{3}\alpha_{n-1}}+5 & (n)' \end{array}\right\}$$

και θα οδηγηθούμε στο αποτέλεσμα: $\alpha_n=2\left(\frac{2}{3}\right)^{n-1}+5\cdot\left(1+\frac{2}{3}+\left(\frac{2}{3}\right)^2+\left(\frac{2}{3}\right)^3+\cdots++\left(\frac{2}{3}\right)^{n-2}\right)=$

$= 2 \cdot \left(\frac{2}{3}\right)^{n-1} + 5 \cdot \frac{1 - \left(\frac{2}{3}\right)^{n-1}}{1 - \frac{2}{3}} = 2 \cdot \left(\frac{2}{3}\right)^{n-1} + 15 \cdot \left(1 - \left(\frac{2}{3}\right)^{n-1}\right)$. Επομένως $\lim\limits_{n \to +\infty} \alpha_n = 15$. ■

Παρόλο που η επαγωγή, ως αποδεικτική μέθοδος μπορεί να υστερεί ως προς την «ευρετικότητά» της και σε πολλές περιπτώσεις να μην παρέχει ιδιαίτερα «κομψές» αποδείξεις, εντούτοις εξακολουθεί να αποτελεί **ισχυρότατο εργαλείο στο οπλοστάσιο του μαθηματικού**. Δεν είναι τυχαίο το γεγονός ότι η πρώτη σκέψη που κάνει ο επίδοξος λύτης μιας άσκησης είναι «μήπως η άσκηση αυτή βγαίνει με επαγωγή». Οι κομψότερες λύσεις είναι συνήθως και οι πιο δύσκολες. Η επαγωγή μπορεί επίσης να συνδυαστεί και με άλλες μεθόδους, ώστε ο λύτης να οδηγηθεί στο σωστό αποτέλεσμα. Η προηγούμενη ενδελεχής αναφορά σε αυτήν καταδεικνύει πόσο πολύτιμο εργαλείο είναι. Και αποτελεί ιδιαίτερο πρόβλημα το γεγονός ότι οι «επαΐοντες»(;) της εκπαίδευσης φρόντισαν να την εξαφανίσουν κυριολεκτικά από τη μέση εκπαίδευση. Όπως εξαφάνισαν τη Γεωμετρία, αλλά και **το μεγαλύτερο τμήμα της ύλης των μαθηματικών, το οποίο διδασκόταν επί δεκαετίες στα γυμνάσια και τα λύκεια**. Το αν πέτυχαν κάτι καλύτερο, αυτό φαίνεται από τα προβλήματα που αντιμετωπίζουν οι πρωτοετείς (και όχι μόνον) φοιτητές των θετικών επιστημών όταν ανακαλύπτουν ότι οι επιτηδευμένες ή μάλλον καλύτερα **διεστραμμένες** φροντιστηριακές ασκήσεις που τους επέτρεψαν να εισαχθούν σε κάποια σχολή δεν έχουν καμία σχέση με τα ίδια τα μαθηματικά!

Παράρτημα Δ΄

Βασικές έννοιες Συνδυαστικής

Δ΄.1 Η προσθετική και η πολλαπλασιαστική αρχή

Με απλά λόγια, η (απαριθμητική) Συνδυαστική ασχολείται με τις μεθόδους υπολογισμού του πλήθους των στοιχείων ενός ή περισσοτέρων συνόλων. Σε γενικές γραμμές στηρίζεται σε δύο απλές αρχές: Την προσθετική αρχή και την πολλαπλασιαστική αρχή.

Η Προσθετική Αρχή: Με λίγα λόγια η προσθετική αρχή μας λέει το εξής «αυτονόητο»: Αν έχουμε n σύνολα $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n$ τα οποία είναι ανά δύο ξένα μεταξύ τους (δηλαδή $\mathrm{A}_i \cap \mathrm{A}_j = \varnothing$ για κάθε $i \neq j$), τότε το πλήθος των στοιχείων της ένωσης $\mathrm{A}_1 \cup \mathrm{A}_2 \cup \ldots \cup \mathrm{A}_n$ ισούται με το άθροισμα των πληθαρίθμων των επί μέρους συνόλων, δηλαδή

$$|\mathrm{A}_1 \cup \mathrm{A}_2 \cup \ldots \cup \mathrm{A}_n| = |\mathrm{A}_1| + |\mathrm{A}_2| + \cdots + |\mathrm{A}_n|$$

ή πιο σύντομα

$$\left|\bigcup_{i=1}^{n} \mathrm{A}_i\right| = \sum_{i=1}^{n} |\mathrm{A}_i|$$

Σημείωση: Αν έχουμε n σύνολα $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n$, τα οποία είναι ανά δύο ξένα, τότε η ένωσή τους λέγεται **ξένη ένωση** και για έμφαση συμβολίζεται με $\mathrm{A}_1 \dot{\cup} \mathrm{A}_2 \dot{\cup} \ldots \dot{\cup} \mathrm{A}_n$ ή πιο σύντομα $\dot{\bigcup}_{i=1}^{n} \mathrm{A}_i$.

Παραδείγματα: 1) Ας υποθέσουμε ότι έχουμε δύο παρέες μαθητών. Η πρώτη αποτελείται από τρεις μαθητές, τους α_1, α_2 και α_3 και η δεύτερη από τους β_1, β_2 και β_3. Θέλουμε να επιλέξουμε δύο μαθητές, οι οποίοι όμως θα πρέπει να ανήκουν στην ίδια παρέα. Έχουμε δύο περιπτώσεις:
α) Οι μαθητές να ανήκουν στην πρώτη παρέα, οπότε και παίρνουμε έτσι το σύνολο $\mathrm{A}_1 = \{\{\alpha_1, \alpha_2\}, \{\alpha_1, \alpha_3\}, \{\alpha_2, \alpha_3\}\}$ και
β) οι μαθητές να ανήκουν στην δεύτερη παρέα, οπότε και παίρνουμε έτσι το σύνολο $\mathrm{A}_2 = \{\{\beta_1, \beta_2\}, \{\beta_1, \beta_3\}, \{\beta_2, \beta_3\}\}$.
Κάθε ένα τα δύο σύνολα περιέχει 3 στοιχεία. Άρα το πλήθος των δυνατών περιπτώσεων είναι ίσο με $|\mathrm{A}_1 \cup \mathrm{A}_2| = |\mathrm{A}_1| + |\mathrm{A}_2| = 3 + 3 = 6$.
2) Να βρεθούν όλα τα ζεύγη (x, y) των ακεραίων με την ιδιότητα $x^2 + y^2 \leq 5$. Αν συμβολίσουμε με S_i το σύνολο $\{(x, y) \mid x^2 + y^2 = i\}$, τότε το ζητούμενο πλήθος είναι ο πληθάριθμος της ξένης ένωσης $\mathrm{S}_0 \dot{\cup} \mathrm{S}_1 \dot{\cup} \mathrm{S}_2 \dot{\cup} \mathrm{S}_3 \dot{\cup} \mathrm{S}_4 \dot{\cup} \mathrm{S}_5$. Παρατηρούμε ότι $\mathrm{S}_0 = \{(0,0)\}$, $\mathrm{S}_1 = \{(1,0), (-1,0), (0,1), (0,-1)\}$, $\mathrm{S}_2 = \{(1,1), (-1,1), (1,-1), (-1,-1)\}$, $\mathrm{S}_3 = \varnothing$, $\mathrm{S}_4 = \{(2,0), (-2,0), (0,2), (0,-2)\}$ και $\mathrm{S}_5 = \{(2,1), (-2,1), (2,-1), (-2,-1), (1,2), (1,-2), (-1,2), (-1,-2)\}$. Επομένως το ζητούμενο πλήθος είναι $1 + 4 + 4 + 0 + 4 + 8 = 21$.

Η Πολλαπλασιαστική Αρχή: Η πολλαπλασιαστική αρχή μας λέει το εξής απλό: Υποθέτουμε ότι μια διαδικασία για να πραγματοποιηθεί απαιτεί n διαδοχικά στάδια, τα οποία συμβολίζουμε με $E_1, E_2, \ldots, E_n$. Αν το στάδιο E_1 μπορεί να πραγματοποιηθεί κατά k_1 τρόπους, το στάδιο E_2 κατά k_2 τρόπους, ... και τέλος το στάδιο E_n κατά k_n τρόπους, τότε η όλη διαδικασία μπορεί να πραγματοποιηθεί κατά

$$k_1 \cdot k_2 \cdots k_n$$

τρόπους.

Παράδειγμα: Ένα πλήρες γεύμα σε κάποιο (ίσως καλό) εστιατόριο περιλαμβάνει:
α) ορεκτικό (στάδιο E_1), **β)** το κυρίως πιάτο (στάδιο E_2) και τέλος **γ)** το γλυκό (στάδιο E_3).
Ο πελάτης έχει να επιλέξει ανάμεσα **3** είδη ορεκτικών ($|E_1| = 3$), **5** είδη κυρίως πιάτων ($|E_2| = 5$) και **2** είδη γλυκών ($|E_3| = 2$). Σύμφωνα με την πολλαπλασιαστική αρχή το πλήθος των διαφορετικών γευμάτων που προσφέρει το εστιατόριο ισούται με $3 \cdot 5 \cdot 2 = 30$.
Στη συνέχεια θα μάθουμε πώς να εφαρμόζουμε αυτές τις απλές αρχές και επιπλέον θα γνωρίσουμε και άλλες αρχές το ίδιο απλές αλλά και το ίδιο σημαντικές.

Δ΄.2 Διατάξεις-μεταθέσεις

Έστω $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$, n διαφορετικά αντικείμενα. ($n \geq 1$). Αν $1 \leq k \leq n$, τότε τίθεται το εξής πρόβλημα: Κατά πόσους τρόπους μπορούμε από τα n αντικείμενα να πάρουμε k και να τα τοποθετήσουμε σε μια σειρά; Το πρόβλημα είναι ισοδύναμο με το εξής: Έχουμε k κελιά. Κατά πόσους τρόπους μπορούμε να τοποθετήσουμε σε αυτά τα κελιά k αντικείμενα από τα n;

Σχήμα 18

Μια τέτοια τοποθέτηση k αντικειμένων από συνολικά n λέγεται **διάταξη n αντικειμένων ανά k**. Το πλήθος των διατάξεων n (αντικειμένων) ανά k ας το συμβολίσουμε με Δ_k^n.
Παρατηρούμε ότι για το 1ο κελί έχουμε n επιλογές. Αφού επιλέξουμε το 1ο απομένουν $n-1$ αντικείμενα. Άρα για το 2ο κελί έχουμε $n-1$ επιλογές. Αφού επιλέξουμε και το 2ο απομένουν $n-2$ αντικείμενα. Άρα για το 3ο κελί έχουμε $n-2$ επιλογές. Τελικά, αν έχουμε επιλέξει τα πρώτα $k-1$ αντικείμενα, τότε απομένουν $n-(k-1) = n-k+1$ αντικείμενα, άρα $n-k+1$ επιλογές για το τελευταίο κελί. Σύμφωνα με την πολλαπλασιαστική αρχή παίρνουμε

$$\Delta_k^n = n(n-1)(n-2)\cdots(n-k+1)$$

Αν $k = n$, το πρόβλημα έγκειται στο κατά πόσους τρόπους μπορούμε n διακεκριμένα αντικείμενα να τα τοποθετήσουμε σε μια σειρά. Μια τέτοια διάταξη όλων των n αντικειμένων λέγεται **μετάθεση των n αντικειμένων**. Αν M_n είναι το πλήθος τους, τότε

$$\mathrm{M}_n = \Delta_n^n = n(n-1)(n-2)\cdots 2\cdot 1 = n!$$

Δ΄.3 Συνδυασμοί

Έστω n αντικείμενα και $k \leq n$. Τίθεται το ερώτημα: Κατά πόσους τρόπους μπορούμε να επιλέξουμε k αντικείμενα από τα n; (Χωρίς όμως να τα διατάξουμε). Το ερώτημα είναι ισοδύναμο με το ερώτημα:«πόσα υποσύνολα με ακριβώς k στοιχεία έχει ένα σύνολο με n στοιχεία;» Κάθε επιλογή k στοιχείων από n λέγεται **συνδυασμός n στοιχείων ανά k**. Έστω Σ_k^n το πλήθος τους. Για να προσδιορίσουμε το Σ_k^n σκεφτόμαστε ως εξής: Κάθε διάταξη n αντικειμένων ανά k πραγματοποιείται σε δύο φάσεις:
1η φάση: Από τα n στοιχεία επιλέγουμε τα k τα οποία θέλουμε να διατάξουμε. Αυτό γίνεται κατά Σ_k^n τρόπους.
2η φάση: Μεταθέτουμε τα k επιλεχθέντα στοιχεία. Αυτό γίνεται κατά $k!$ τρόπους.
Σύμφωνα με την πολλαπλασιαστική αρχή, το πλήθος Δ_k^n των διατάξεων n στοιχείων ανά k ισούται με $\Sigma_k^n \cdot k!$. Επομένως

$$\Sigma_k^n = \frac{\Delta_k^n}{k!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \binom{n}{k}$$

Το σύμβολο $\Sigma_k^n \cdot k!$ έχει έννοια ακόμα και αν κάποιο από τα n, k είναι μηδέν ή το k να είναι μεγαλύτερο του n. Αν $k = 0$, τότε έχουμε **ακριβώς μία** επιλογή: να μην πάρουμε κανένα στοιχείο. Ισοδύναμα να πάρουμε το $\varnothing$. Αυτό μπορεί να συμβεί ακόμα και αν $n = 0$. (Το κενό σύνολο έχει ένα ακριβώς υποσύνολο: το ίδιο

το κενό). Αυτό συμπίπτει με τον ορισμό του $\binom{n}{0} = 1$. Αν τώρα $n < k$, τότε δεν έχουμε **καμία** επιλογή. Δεν μπορούμε από λιγότερα στοιχεία να πάρουμε περισσότερα. Και στην περίπτωση αυτή ο αριθμός Σ_k^n συμπίπτει με το σύμβολο $\binom{n}{k} = 0$. Άρα, σε κάθε περίπτωση

$$\Sigma_k^n = \binom{n}{k}$$

Παρατηρήσεις: 1) Η συνδυαστική ερμηνεία του γεγονότος ότι $\binom{n}{k} = \binom{n}{n-k}$ είναι η εξής: Όταν από ένα σύνολο Α με n στοιχεία θεωρήσουμε ένα υποσύνολό του Χ με k στοιχεία, τότε αυτομάτως έχουμε ορίσει το συμπλήρωμα $\mathrm{A} \setminus \mathrm{X}$ του Χ στο Α, το οποίο (είναι μοναδικό) και περιέχει $n-k$ στοιχεία. Ισχύει προφανώς και το αντίστροφο: αν επιλέξουμε ένα υποσύνολο Υ του Α με $n-k$ στοιχεία, τότε το $\mathrm{X} = \mathrm{A} \setminus \mathrm{Y}$ αποτελείται ακριβώς από k στοιχεία και προφανώς $\mathrm{A} \setminus \mathrm{X} = \mathrm{A} \setminus (\mathrm{A} \setminus \mathrm{Y}) = \mathrm{Y}$.
Αν λοιπόν $\mathcal{A} \subseteq \mathcal{P}(\mathrm{A})$ είναι η συλλογή των υποσυνόλων του Α με k στοιχεία και $\mathcal{B}$ η συλλογή των υποσυνόλων του Α με $n-k$ στοιχεία, τότε η απεικόνιση $f : \mathcal{A} \to \mathcal{B}$, με $f(\mathrm{X}) = \mathrm{A} \setminus \mathrm{X}$ είναι 1-1 και επί. Άρα $|\mathcal{A}| = |\mathcal{B}|$, δηλαδή

$$\binom{n}{k} = \binom{n}{n-k}$$

2) Στην προηγούμενη παρατήρηση υποκρίπτεται και μια άλλη σημαντική αρχή της Συνδυαστικής. **Η Αρχή της αμφιμονοσήματης αντιστοιχίας**. Με απλά λόγια, αν Α και Β είναι δύο σύνολα και υπάρχει $f : \mathrm{A} \to \mathrm{B}$, η οποία είναι 1-1 και επί, τότε $|\mathrm{A}| = |\mathrm{B}|$. Η αρχή της αμφιμονοσήμαντης αντιστοιχίας εφαρμόζεται όταν δεν μπορούμε να υπολογίσουμε εύκολα το πλήθος των στοιχείων του Α, ενώ μπορούμε να υπολογίσουμε πιο εύκολα το πλήθος των στοιχείων του Β. Έτσι, μέσω της αντιστοιχίας f το πρόβλημα του υπολογισμού του $|\mathrm{A}|$ ανάγεται στο πρόβλημα του υπολογισμού του $|\mathrm{B}|$.

Εφαρμογή Δ΄.1. (Συνδυαστική απόδειξη του διωνύμου του Newton) Για κάθε θετικό ακέραιο n ισχύει η ταυτότητα:

$$(\alpha+\beta)^n = \sum_{k=0}^{n} \binom{n}{k} \alpha^k \beta^{n-k}$$

Απόδειξη: Γράφουμε το $(\alpha+\beta)^n$ ως εξής:

$$(\alpha+\beta)^n = \underbrace{\overset{1^{\eta}\text{ παρένθεση}}{(\alpha+\beta)} \quad \overset{2^{\eta}\text{ παρένθεση}}{(\alpha+\beta)} \quad \overset{3^{\eta}\text{ παρένθεση}}{(\alpha+\beta)} \quad \cdots \quad \overset{n\text{-στή παρένθεση}}{(\alpha+\beta)}}_{n\text{ παρενθέσεις}}$$

Όταν εκτελούμε τις πράξεις μεταξύ των παρενθέσεων, με βάση την επιμεριστική ιδιότητα, τότε για να εμφανιστεί ο όρος $\alpha^k\beta^{n-k}$ θα πρέπει κάθε φορά να επιλέγουμε από τις n παρενθέσεις τις k από τις οποίες θα πάρουμε το α. Από τις υπόλοιπες αναγκαστικά θα πάρουμε το β. Από κάθε τέτοια επιλογή παίρνουμε 1 που το υπολογίζουμε στον συντελεστή του $\alpha^k\beta^{n-k}$. Εφόσον έχουμε n παρενθέσεις και επιλέγουμε κάθε φορά k από τις οποίες θα πάρουμε το α, αθροίζοντας για όλες αυτές τις επιλογές, ο συντελεστής του $\alpha^k\beta^{n-k}$ στο ανάπτυγμα του $(\alpha+\beta)^n$ θα πρέπει να είναι ίσος με $\binom{n}{k}$. ■

Εφαρμογή Δ΄.2. Να αποδείξετε συνδυαστικά τον τύπο: $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$.

Απόδειξη: Το πρώτο μέλος μετράει τα υποσύνολα ενός συνόλου με n στοιχεία. Πράγματι, το $\binom{n}{0} = 1$ ισούται με το πλήθος των υποσυνόλων με 0 στοιχεία (δηλαδή μόνον το κενό), το $\binom{n}{1} = n$ με το πλήθος των υποσυνόλων με ένα στοιχείο (μονοσύνολα), το $\binom{n}{2}$ με το πλήθος των υποσυνόλων με δύο στοιχεία κ.ο.κ.

Δηλαδή το πρώτο μέλος ισούται με το πλήθος των υποσυνόλων ενός συνόλου με n στοιχεία. Δηλαδή, αν $\mathrm{A} = \{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n\}$, τότε το πρώτο μέλος ισούται με τον πληθάριθμο του $\mathcal{P}(\mathrm{A})$. Για να υπολογίσουμε τον $|\mathcal{P}(\mathrm{A})|$ σκεπτόμαστε ως εξής: Θεωρούμε μια σταθερή διάταξη $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ των στοιχείων του Α. Τότε για κάθε υποσύνολο Χ του Α ορίζουμε ένα διάνυσμα $f(\mathrm{X}) = (x_1, x_2, \ldots, x_n)$ ως εξής: $x_i = \begin{cases} 1, & \text{αν } \alpha_i \in \mathrm{X} \\ 0, & \text{αν } \alpha_i \notin \mathrm{X} \end{cases}$
Κάθε τέτοιο διάνυσμα με στοιχεία από το $\{0, 1\}$ ορίζει με τη σειρά του ένα μοναδικό υποσύνολο Χ του Α, δηλαδή είναι εικόνα του Χ. Για παράδειγμα, υποθέστε ότι $\mathrm{A} = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. Το διάνυσμα $(1, 1, 0, 1)$ ορίζει το υποσύνολο $\{\alpha_1, \alpha_2, \alpha_4\}$, το διάνυσμα $(0, 0, 0, 0)$ ορίζει το κενό σύνολο, το διάνυσμα $(0, 1, 1, 0)$ ορίζει το υποσύνολο $\{\alpha_2, \alpha_3\}$, το διάνυσμα $(1, 1, 1, 1)$ ορίζει το $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \mathrm{A}$.
Επανερχόμαστε στη γενική περίπτωση: Από τα παραπάνω καθίσταται φανερό (αρχή της αμφιμονοσήμαντης αντιστοιχίας) ότι το πλήθος των υποσυνόλων του Α ισούται με το πλήθος των διανυσμάτων της μορφής $(x_1, x_2, \ldots, x_n)$, όπου $x_i \in \{0, 1\}$. Πόσα είναι αυτά τα διανύσματα; Για το x_1 έχουμε δύο επιλογές (0 ή 1), για το x_2 πάλι δύο επιλογές,... και για το x_n επίσης δύο επιλογές. Σύμφωνα με την πολλαπλασιαστική αρχή έχουμε $\underbrace{2 \cdot 2 \cdots 2}_{n \text{ φορές}} = 2^n$ επιλογές. ■

Δ΄.4 Επαναληπτικές διατάξεις-Επαναληπτικοί συνδυασμοί

Τις **επαναληπτικές διατάξεις** τις έχουμε ήδη χρησιμοποιήσει στην προηγούμενη εφαρμογή. Μια επαναληπτική διάταξη n αντικειμένων ανά k είναι η τοποθέτηση σε μια σειρά k θέσεων ή ισοδύναμα σε k κελιά κάποιων από τα n αντικείμενα **με δυνατότητα επανάληψης** καθενός από τα αντικείμενα για περισσότερες από μία φορά. Εδώ μπορεί το k να είναι μεγαλύτερο του n.
Έτσι, αν το σύνολο των αντικειμένων είναι π.χ. το $\{1, 2, 3\}$ και $k = 4$, τότε οι τοποθετήσεις 1132, 2221, 3222 είναι κάποιες από τις επαναληπτικές διατάξεις 3 αντικειμένων ανά 4. Δηλαδή οι επαναληπτικές διατάξεις n αντικειμένων ανά k είναι όλες οι πεπερασμένες ακολουθίες μήκους k με όρους-στοιχεία από ένα σύνολο με n στοιχεία. Έστω $\boldsymbol{\mathrm{ΕΔ}_k^n}$ το πλήθος των επαναληπτικών διατάξεων n αντικειμένων ανά k. Για την πρώτη θέση έχουμε n επιλογές, αλλά και για τη δεύτερη, την τρίτη κτλ έχουμε πάλι n επιλογές, γιατί επιτρέπονται επαναλήψεις. Σύμφωνα με την πολλαπλασιαστική αρχή έχουμε

$$\mathrm{ΕΔ}_k^n = \underbrace{n \cdot n \cdot n \cdots n}_{k \text{ φορές}} = n^k$$

Τώρα, ένας **επαναληπτικός συνδυασμός** n αντικειμένων ανά k (και εδώ το k μπορεί να είναι μεγαλύτερο του n) είναι μια επιλογή k αντικειμένων από τα n, **με δυνατότητα επανάληψης αλλά χωρίς να μας ενδιαφέρει η διάταξή τους**. Έστω $\boldsymbol{\mathrm{ΕΣ}_k^n}$ το πλήθος των επαναληπτικών συνδυασμών n αντικειμένων ανά k.

Πρόταση Δ΄.3. Ισχύει η σχέση: $\mathrm{ΕΣ}_k^n = \binom{n+k-1}{k}$.

1η Απόδειξη: Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι το σύνολο των n αντικειμένων είναι το $\{1, 2, 3, \ldots, n\}$. Αφού επιλέξουμε k αριθμούς, ενδεχομένως με επαναλήψεις, από το σύνολο $\{1, 2, 3, \ldots, n\}$, τους διατάσσουμε κατ' αύξουσα σειρά. Έτσι παίρνουμε ένα **μοναδικό** διάνυσμα $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, όπου $\alpha_i \in \{1, 2, \ldots, n\}$ για κάθε $i = 1, 2, \ldots, k$ και $\alpha_1 \leq \alpha_2 \leq \alpha_3 \leq \cdots \leq \alpha_k$. Το ίσον (=) στη σχέση $\leq$ επιτρέπει την ενδεχόμενη επανάληψη των αντικειμένων. Από το διάνυσμα $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ ορίζεται ένα **μοναδικό** διάνυσμα $(\beta_1, \beta_2, \ldots, \beta_k)$ ως εξής: Θέτουμε $\beta_1 = \alpha_1$, $\beta_2 = \alpha_2 + 1$, $\beta_3 = \alpha_3 + 2$ και τελικώς $\beta_k = \alpha_k + k - 1$. Δηλαδή, $\beta_i = \alpha_i + i - 1$ για κάθε $i = 1, 2, \ldots, k$. Παρατηρούμε ότι $\beta_{i+1} - \beta_i = \alpha_{i+1} + (i+1) - 1 - (\alpha_i + i - 1) = \alpha_{i+1} - \alpha_i + 1 \geq 1$, γιατί $\alpha_{i+1} - \alpha_i \geq 0$. Επομένως $\beta_{i+1} > \beta_i$, για κάθε $i = 1, 2, \ldots, k-1$. Η ελάχιστη τιμή που μπορεί να πάρει το $\beta_1 = \alpha_1$ είναι το 1 και η μέγιστη τιμή που μπορεί να πάρει το $\beta_k = \alpha_k + k - 1$ είναι $n + k - 1$. Επειδή στο νέο διάνυσμα $(\beta_1, \beta_2, \ldots, \beta_k)$ δεν έχουμε ισότητες, αυτό καθορίζει έναν **μοναδικό** (απλό) συνδυασμό $n+k-1$ αντικειμένων, παρμένων από το σύνολο $\{1, 2, 3, \ldots, n+k-1\}$ ανά k. Ισχύει και το αντίστροφο: Αν $(\beta_1, \beta_2, \ldots, \beta_k)$ είναι το διάνυσμα που αντιστοιχεί

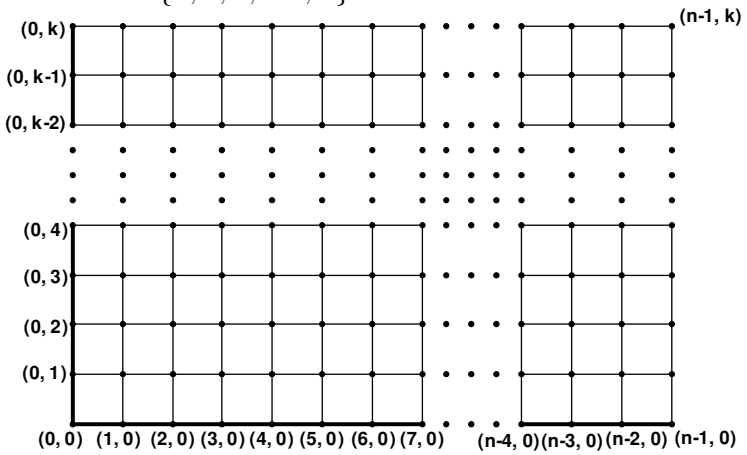
σ' έναν απλό συνδυασμό των $n+k-1$ αριθμών $1,2,3,\ldots,n+k-1$ ανά k, με $\beta_1<\beta_2<\cdots<\beta_k$, τότε μπορούμε να **ανακτήσουμε** το αρχικό διάνυσμα $(\alpha_1,\alpha_2,\ldots,\alpha_k)$ από το σύνολο των αριθμών $1,2,3,\ldots,n$, με $\alpha_1\le\alpha_2\le\cdots\le\alpha_k$ ως εξής: Θέτουμε $\alpha_1=\beta_1$, $\alpha_2=\beta_2-1$, $\alpha_3=\beta_3-2$ και γενικά $\alpha_i=\beta_i-i+1$, για κάθε $i=1,2,\ldots,k$. Παρατηρούμε ότι $\alpha_{i+1}-\alpha_i=\beta_{i+1}-(i+1)+1-(\beta_i-i+1)=\beta_{i+1}-\beta_i-1\ge 0$, γιατί $\beta_{i+1}>\beta_i$, για κάθε $i=1,2,\ldots,k$. Η ελάχιστη τιμή του $\alpha_1=\beta_1$ είναι το 1 και η μέγιστη τιμή του $\alpha_k=\beta_k-k+1$ είναι $(n+k-1)-k+1=n$. Άρα όντως το διάνυσμα $(\alpha_1,\alpha_2,\ldots,\alpha_k)$ αντιστοιχεί σε έναν επαναληπτικό συνδυασμό n αντικειμένων ανά k. Σύμφωνα με την αρχή της αμφιμονοσήμαντης αντιστοιχίας, το πλήθος των επαναληπτικών συνδυασμών n αντικειμένων ανά k ισούται με το πλήθος των απλών συνδυασμών $n+k-1$ αντικειμένων ανά k. Επομένως $\text{ΕΣ}_k^n=\binom{n+k-1}{k}$. ■

2η Απόδειξη: Από όλους τους ΕΣ_k^n επαναληπτικούς συνδυασμούς των n αντικειμένων $\alpha_1,\alpha_2,\ldots,\alpha_n$ υπολογίζουμε πόσες συνολικά φορές έχει εμφανιστεί ένα συγκεκριμένο αντικείμενο, π.χ. το α_1. Έστω λ ο αριθμός αυτός. Λόγω συμμετρίας, ο αριθμός αυτός είναι ο ίδιος για όλα τα n αντικείμενα. Αθροιστικά λοιπόν όλα τα αντικείμενα, σε όλους τους ΕΣ_k^n επαναληπτικούς συνδυασμούς εμφανίζονται $n\lambda$ φορές. Επειδή σε κάθε έναν από τους ΕΣ_k^n επαναληπτικούς συνδυασμούς εμφανίζονται (ενδεχομένως με επαναλήψεις) k αντικείμενα, θα έχουμε $n\lambda=k\cdot\text{ΕΣ}_k^n\Leftrightarrow\lambda=\dfrac{k}{n}\cdot\text{ΕΣ}_k^n$. Αν τώρα από κάθε επαναληπτικό συνδυασμό που περιέχει το α_1 αφαιρέσουμε το στοιχείο αυτό μία μόνον φορά, θα πάρουμε όλους τους επαναληπτικούς συνδυασμούς n αντικειμένων ανά $k-1$. (Σε αυτούς μπορεί το α_1 να επανεμφανίζεται). Σύμφωνα με το προηγούμενο επιχείρημα, στους τελευταίους αυτούς ΕΣ_{k-1}^n επαναληπτικούς συνδυασμούς το α_1 θα εμφανίζεται συνολικά $\lambda'=\dfrac{k-1}{n}\cdot\text{ΕΣ}_{k-1}^n$ φορές. Επειδή οι ΕΣ_{k-1}^n συνδυασμοί προέκυψαν με αφαίρεση ενός α_1, το σύνολο λ των εμφανίσεων του α_1 σε όλους τους ΕΣ_k^n επαναληπτικούς συνδυασμούς θα ισούται με $\lambda=\lambda'+\text{ΕΣ}_{k-1}^n\Leftrightarrow\dfrac{k}{n}\cdot\text{ΕΣ}_k^n=\dfrac{k-1}{n}\cdot\text{ΕΣ}_{k-1}^n+\text{ΕΣ}_{k-1}^n=\dfrac{n+k-1}{n}\cdot\text{ΕΣ}_{k-1}^n\Leftrightarrow\text{ΕΣ}_k^n=\dfrac{n+k-1}{k}\cdot\text{ΕΣ}_{k-1}^n$. Η τελευταία αναδρομική σχέση μας οδηγεί στο αποτέλεσμα $\text{ΕΣ}_k^n=\dfrac{(n+k-1)(n+k-2)\cdots(n+1)}{k(k-2)\cdots 2}\cdot\text{ΕΣ}_1^n$. Αλλά $\text{ΕΣ}_1^n=n$, οπότε

$$\text{ΕΣ}_k^n=\frac{n(n+1)\cdots(n+k-2)(n+k-1)}{k!}=\binom{n+k-1}{k}$$

■

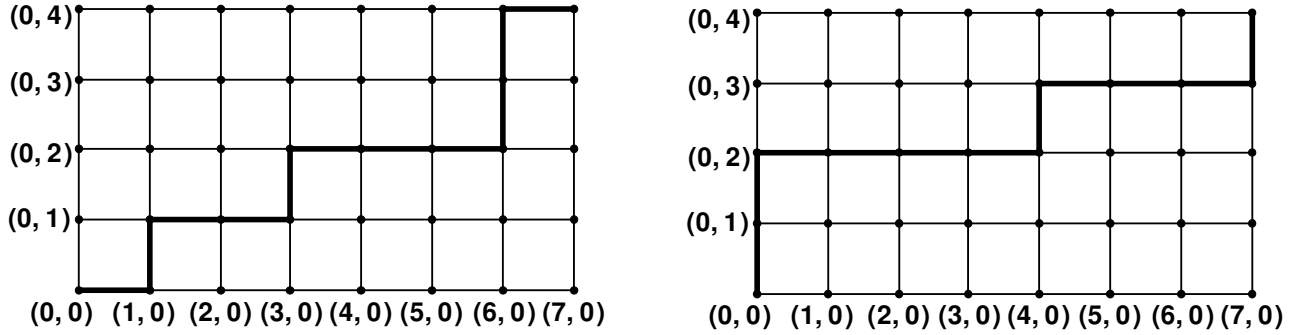
3η Απόδειξη: (Γεωμετρική) Θεωρούμε το πλέγμα που ορίζεται από τα σημεία του επιπέδου με ακέραιες συντεταγμένες (lattice-points). Θα περιοριστούμε στα σημεία που έχουν τετμημένη από το σύνολο $\{0,1,\ldots,n-1\}$ και τεταγμένη από το σύνολο $\{0,1,2,\ldots,k\}$.



Σχήμα 19

Υποθέτουμε ότι ένας δρόμος ξεκινά από το σημείο $(0,0)$ και καταλήγει στο σημείο $(n-1,k)$ περνώντας από τα ενδιάμεσα lattice-points. Κάθε φορά μπορούμε να κινηθούμε είτε δεξιά κατά 1 μονάδα είτε πάνω κατά 1 μονάδα και πάλι. Το ερώτημα είναι: «πόσοι τέτοιοι δρόμοι υπάρχουν;»
Για παράδειγμα, αν $n=8$ και $k=4$, τότε μπορούμε να θεωρήσουμε δύο διαφορετικούς δρόμους, όπως

στο επόμενο σχήμα:



Σχήμα 20

Κάθε τέτοιος δρόμος αποτελείται από $n-1$ οριζόντια και k κατακόρυφα μοναδιαία διαστήματα. Συνολικά κάποιος πρέπει να διασχίσει $n+k-1$ μοναδιαία διαστήματα για να βρεθεί από το σημείο $(0,0)$ στο σημείο $(n-1,k)$. Δηλαδή από κάθε σημείο έχει δύο μόνον επιλογές: Ή να κινηθεί δεξιά κατά 1 ή προς τα πάνω κατά 1. Αν θέσουμε 0 για τα οριζόντια διαστήματα και 1 για τα κατακόρυφα, τότε κάθε δρόμος αντιστοιχεί σε μια ακολουθία μήκους $n+k-1$ με στοιχεία 0 ή 1. Έτσι, στο αριστερό σχήμα αντιστοιχεί η ακολουθία 01001000110 και στο δεξιό σχήμα η ακολουθία 11000010001. Γενικά λοιπόν το πρόβλημα ανάγεται στο να επιλέξουμε από τις $n+k-1$ θέσεις της ακολουθίας, αυτές στις οποίες θα βάλουμε 1. Στις υπόλοιπες αναγκαστικά θα βάλουμε 0. Επειδή υπάρχουν k κατακόρυφα τμήματα, είμαστε υποχρεωμένοι να επιλέξουμε από τις $n+k-1$ θέσεις, ακριβώς k θέσεις στις οποίες θα βάλουμε 1. Αυτό γίνεται κατά $\binom{n+k-1}{k}$ τρόπους.

Τώρα θα μετρήσουμε τους δρόμους διαφορετικά. Επιλέγουμε από τις n κατακόρυφες ευθείες με τετμημένες $\{0,1,2,\ldots,n-1\}$ εκείνες στις οποίες υπάρχουν σημεία στα οποία θα κινηθούμε προς τα πάνω. Έτσι, στο αριστερό σχήμα κίνηση προς τα πάνω γίνεται στις τετμημένες $1,3$ και 6. Κάθε φορά που κινούμαστε προς τα πάνω αυτό ισοδυναμεί με την εμφάνιση της ίδιας τετμημένης ακόμα 1 φορά. Έτσι, στο αριστερό σχήμα η τετμημένη 1 εμφανίζεται 1 φορά, η 3 εμφανίζεται 1 φορά και η 6 εμφανίζεται 2 φορές. Αν προσθέσουμε το συνολικό πλήθος των κατακόρυφων κινήσεων θα πάρουμε φυσικά $1+1+2=4$, όσα και τα κατακόρυφα τμήματα. Στο δεύτερο σχήμα η μηδενική τετμημένη εμφανίζεται 2 φορές, η τετμημένη 4 εμφανίζεται 1 φορά και τέλος, η τετμημένη 7 εμφανίζεται 1 φορά. (Και πάλι $2+1+1=4$, αναγκαστικά). Πρόκειται λοιπόν για **το πλήθος των επαναληπτικών συνδυασμών των n τετμημένων $\{0,1,2,\ldots,n-1\}$ ανά k**. Επειδή οι δύο μετρήσεις πρέπει να δίνουν το ίδιο αποτέλεσμα, συνάγουμε ότι το πλήθος των επαναληπτικών συνδυασμών n αντικειμένων ανά k ισούται με $\binom{n+k-1}{k}$. ■

Συμβολισμός: Το πλήθος των επαναληπτικών συνδυασμών n αντικειμένων ανά k συμβολίζεται συνήθως με $\left(\binom{n}{k}\right)$.

Άσκηση 133. (i) Πόσες διατεταγμένες n-άδες $(x_1,x_2,\ldots,x_n)$ μη αρνητικών ακεραίων υπάρχουν με την ιδιότητα $x_1+x_2+\cdots+x_n=k$;
(ii) Πόσες διατεταγμένες n-άδες $(x_1,x_2,\ldots,x_n)$ μη αρνητικών ακεραίων υπάρχουν με την ιδιότητα x_1+ $+x_2+\cdots+x_n\leq k$;
(iii) Πόσες διατεταγμένες πεντάδες (x_1,x_2,x_3,x_4,x_5) θετικών ακεραίων υπάρχουν με την ιδιότητα x_1+x_2+ $+x_3+x_4+x_5=17$;
Λύση: (i) Κάθε n-άδα αντιστοιχεί στην εμφάνιση της 1ης θέσης x_1 φορές, της 2ης x_2 φορές, κτλ, και της n-στής θέσης x_n φορές. Πρόκειται λοιπόν για το πλήθος των επαναληπτικών συνδυασμών των n θέσεων ανά k. Το αποτέλεσμα είναι $\binom{n+k-1}{k}$.
(ii) Αν $x_1+x_2+\cdots+x_n\leq k$ εισάγουμε μια νέα μεταβλητή $x_{n+1}=k-x_1-x_2-\cdots-x_n\geq 0$. Επομένως το πρόβλημα ανάγεται στον προσδιορισμό του πλήθους των $(n+1)$-άδων $(x_1,x_2,\ldots,x_n,x_{n+1})$ με x_1+x_2+

$+\cdots+x_n+x_{n+1}=k$. Αποτέλεσμα: $\binom{n+1+k-1}{k}=\binom{n+k}{k}$.
(iii) Εφόσον $x_i>0$, θα έχουμε $y_i=x_i-1\geq 0$, για κάθε $i=1,2,3,4,5$. Επομένως $x_1+x_2+x_3+x_4+x_5=$ $=17\Leftrightarrow(x_1-1)+(x_2-1)+(x_3-1)+(x_4-1)+(x_5-1)=12\Leftrightarrow y_1+y_2+y_3+y_4+y_5=12$. Αποτέλεσμα: $\binom{5+12-1}{12}=\binom{16}{12}=\binom{16}{4}=\frac{16\cdot15\cdot14\cdot13}{1\cdot2\cdot3\cdot4}=\frac{2\cdot15\cdot14\cdot13}{3}=10\cdot14\cdot13=1820$. ■

Άσκηση 134. (i) Πόσα μονώνυμα στις n μεταβλητές x_1, x_2, …, x_n βαθμού $r\geq 0$ υπάρχουν;
(ii) Πόσα μονώνυμα στις n μεταβλητές x_1, x_2, …, x_n το πολύ βαθμού $r\geq 0$ υπάρχουν;
Λύση: (i) Ένα τέτοιο μονώνυμο είναι της μορφής $x_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}$, όπου $r_i\geq 0$ και $r_1+r_2+\cdots+r_n=r$. Άρα πρόκειται για επαναληπτικούς συνδυασμούς n αντικειμένων ανά r, δηλαδή $\binom{n+r-1}{r}$.

(ii) 1ος τρόπος: Τα μονώνυμα είναι βαθμού $s\leq r$ είναι $\binom{n+s-1}{s}$ το πλήθος. Επομένως ο ζητούμενος αριθμός είναι $\sum_{s=0}^{r}\binom{n+s-1}{s}$. Για $r=0$ παίρνουμε το σταθερό μονώνυμο 1. Αν $r=1$ παίρνουμε $1+\binom{n+1-1}{1}=1+n$, για $r=2$ παίρνουμε $1+n+\binom{n+2-1}{2}=n+1+\frac{(n+1)n}{2}=(n+1)\left(1+\frac{n}{2}\right)=$ $=\frac{(n+2)(n+1)}{2}$.
Δημιουργείται η εικασία ότι ο ζητούμενος αριθμός μπορεί να είναι ίσος με

$$\frac{(n+r)(n+r-1)(n+r-2)\cdots(n+1)}{r!}=\binom{n+r}{r}.$$

Μέχρι $r=2$ το έχουμε αποδείξει. Υποθέτουμε ότι $\sum_{s=0}^{r}\binom{n+s-1}{s}=\binom{n+r}{r}$. Τότε έχουμε:
$\sum_{s=0}^{r+1}\binom{n+s-1}{s}=\sum_{s=0}^{r}\binom{n+s-1}{s}+\binom{n+r}{r+1}\underset{\substack{\text{επαγωγική}\\ \text{υπόθεση}}}{=}\binom{n+r}{r}+\binom{n+r}{r+1}=\binom{n+r+1}{r+1}$, από το τρίγωνο του Pascal.
2ος τρόπος: Όπως είδαμε στο (ii) της προηγούμενης άσκησης, ο ζητούμενος αριθμός ισούται με το πλήθος των n-άδων μη αρνητικών ακεραίων με άθροισμα μικρότερο ή ίσο του r και με την εισαγωγή νέας μεταβλητής ο αριθμός αυτός ισούται με το πλήθος των $(n+1)$-άδων με άθροισμα ακριβώς r. Δηλαδή με $\binom{n+r}{r}$. ■

Δ΄.5 Πολυωνυμικοί συντελεστές

Οι συντελεστές $\binom{n}{k}$ που εμφανίζονται στο ανάπτυγμα του $(x_1+x_2)^n$ λέγονται διωνυμικοί συντελεστές. Ας γενικεύσουμε το πρόβλημα: Στο ανάπτυγμα του $(x_1+x_2+\cdots x_k)^n$ θα εμφανιστούν μονώνυμα της μορφής $x_1^{r_1}x_2^{r_2}\cdots x_k^{r_k}$, όπου $r_1+r_2+\cdots r_k=n$. Ποιος είναι ο συντελεστής ενός τέτοιου μονωνύμου;

Πρόταση Δ΄.4. Ο συντελεστής του $x_1^{r_1}x_2^{r_2}\cdots x_k^{r_k}$ στο ανάπτυγμα του $(x_1+x_2+\cdots x_k)^n$ είναι ίσος με

$$\binom{n}{r_1,r_2,\ldots,r_k}:=\frac{n!}{r_1!r_2!\cdots r_k!},$$

όπου φυσικά $r_1+r_2+\cdots+r_k=n$.
Απόδειξη: Ακολουθούμε την ίδια τακτική με τη συνδυαστική απόδειξη του διωνύμου του Newton. Γράφουμε το $(x_1+x_2+\cdots+x_k)^n$ ως εξής:

$$(x_1+x_2+\cdots+x_k)^n=$$
$$=\underbrace{\overset{1^{\eta}\text{ παρένθεση}}{(x_1+x_2+\cdots+x_k)}\quad\overset{2^{\eta}\text{ παρένθεση}}{(x_1+x_2+\cdots+x_k)}\quad\overset{3^{\eta}\text{ παρένθεση}}{(x_1+x_2+\cdots+x_k)}\quad\cdots\quad\overset{n\text{-στή παρένθεση}}{(x_1+x_2+\cdots+x_k)}}_{n\text{ παρενθέσεις}}$$

Για να πάρουμε r_1 φορές το x_1 θα πρέπει να επιλέξουμε από τις n παρενθέσεις τις r_1 από τις οποίες θα πάρουμε το x_1. Αυτό γίνεται κατά $\binom{n}{r_1}$ τρόπους. Από τις εναπομείνασες $n-r_1$ παρενθέσεις θα επιλέξουμε τις r_2, από τις οποίες θα πάρουμε το x_2, κατά $\binom{n-r_1}{r_2}$ τρόπους. Από τις εναπομείνασες $n-r_1-r_2$ παρενθέσεις θα επιλέξουμε κατά $\binom{n-r_1-r_2}{r_2}$ τρόπους τις r_3, από τις οποίες θα πάρουμε το x_3. Προχωρώντας κατ' αυτόν τον τρόπο, φτάνουμε στο σημείο στο οποίο έχουμε ήδη επιλέξει, κατά $\binom{n-r_1-r_2-\cdots-r_{k-2}}{r_{k-1}}$ τρόπους, από τις $n-r_1-r_2-\cdots-r_{k-2}$ τις r_{k-1} παρενθέσεις από τις οποίες θα πάρουμε το x_{k-1}. Απομένουν $n-r_1-r_2-\cdots r_{k-1}=r_k$ παρενθέσεις από τις οποίες δεν έχουμε άλλη επιλογή από το να πάρουμε το x_k. Σύμφωνα με την πολλαπλασιαστική αρχή, ο συντελεστής του $x_1^{r_1}x_2^{r_2}\cdots x_k^{r_k}$ είναι $\binom{n}{r_1}\binom{n-r_1}{r_2}\cdots\binom{n-r_1-r_2-\cdots-r_{k-2}}{r_{k-1}} = \frac{n!}{r_1!\cancel{(n-r_1)!}}\cdot\frac{\cancel{(n-r_1)!}}{r_2!\cancel{(n-r_1-r_2)!}}\cdot \frac{\cancel{(n-r_1-r_2)!}}{r_3!\cancel{(n-r_1-r_2-r_3)!}}\cdots\frac{(n-r_1-r_2-\cdots-r_{k-2})!}{r_{k-1}!(n-r_1-r_2-\cdots-r_{k-2}-r_{k-1})!} \underset{n-r_1-r_2-\cdots-r_{k-1}=r_k}{=} \frac{n!}{r_1!r_2!\cdots r_k!}$. ■

Δ΄.6 Αρχή του εγκλεισμού-αποκλεισμού

Θεώρημα Δ΄.5. (Αρχή του εγκλεισμού) Έστω $A_1, A_2, \ldots, A_n$ σύνολα. Τότε ισχύει ο ακόλουθος τύπος για το πλήθος των στοιχείων της ένωσης $A_1 \cup A_2 \cup \cdots \cup A_n$.

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n}|A_i| - \sum_{1\le i_1<i_2\le n}|A_{i_1}\cap A_{i_2}| + \sum_{1\le i_1<i_2<i_3\le n}|A_{i_1}\cap A_{i_2}\cap A_{i_3}| - \cdots + $$
$$+(-1)^{n-2}\sum_{1\le i_1<i_2<\cdots<i_{n-1}\le n}|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_{n-1}}| + (-1)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n|. \quad (1)$$

1η Απόδειξη: Ένα στοιχείο της ένωσης $A_1 \cup A_2 \cup \cdots \cup A_n$ θα ανήκει σε ακριβώς k από τα n σύνολα $A_1, A_2, \ldots, A_n$, όπου $1 \le k \le n$.

Στο άθροισμα $\sum_{i=1}^{n}|A_i|$ μετριέται ακριβώς k φορές, στο άθροισμα $\sum_{1\le i_1<i_2\le n}|A_{i_1}\cap A_{i_2}|$ μετριέται $\binom{k}{2}$ φορές, στο άθροισμα $\sum_{1\le i_1<i_2<i_3\le n}|A_{i_1}\cap A_{i_2}\cap A_{i_3}|$ μετριέται $\binom{k}{3}$ φορές κ.ο.κ.

Άρα στο δεύτερο μέλος της αποδεικτέας σχέσης μετριέται ακριβώς

$$k - \binom{k}{2} + \binom{k}{3} - \cdots (-1)^{k-1}\binom{k}{k}$$

φορές. Αλλά $k - \binom{k}{2} + \binom{k}{3} - \cdots (-1)^{k-1}\binom{k}{k} = 1 - 1 + \binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \cdots (-1)^{k-1}\binom{k}{k} = 1 - \left(\binom{k}{0} - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \cdots (-1)^k\binom{k}{k}\right) = 1-(1-1)^k = 1$, δηλαδή ακριβώς **μία** φορά. ■

2η Απόδειξη: Θα εφαρμόσουμε επαγωγή επί του n. Για $n=1$ είναι τετριμμένο, ενώ για $n=2$ ο τύπος $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ είναι αληθής γιατί στο άθροισμα $|A_1| + |A_2|$ το πλήθος των στοιχείων της τομής $A_1 \cap A_2$ μετριέται δύο φορές και πρέπει να αφαιρεθεί. Υποθέτουμε ότι ο τύπος (1) ισχύει για n σύνολα. Θα αποδείξουμε ότι ισχύει και για $n+1$. Έστω λοιπόν $A_1, A_2, \ldots, A_n, A_{n+1}$, $n+1$ σύνολα. Τότε έχουμε: $A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1} = (A_1 \cup A_2 \cup \cdots \cup A_n) \cup A_{n+1}$. Επομένως $|A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}| = |(A_1\cup A_2\cup\cdots\cup A_n)\cup A_{n+1}| = |A_1\cup A_2\cup\cdots\cup A_n| + |A_{n+1}| - |(A_1\cup A_2\cup\cdots\cup A_n)\cap A_{n+1}| = |A_1\cup A_2\cup\cdots\cup A_n| + |A_{n+1}| - |(A_1\cap A_{n+1})\cup(A_2\cap A_{n+1})\cup\cdots\cup(A_n\cap A_{n+1})| = \sum_{i=1}^{n}|A_i| - \sum_{1\le i_1<i_2\le n}|A_{i_1}\cap A_{i_2}| + \sum_{1\le i_1<i_2<i_3\le n}|A_{i_1}\cap A_{i_2}\cap A_{i_3}| - \cdots + (-1)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n| + |A_{n+1}| - \Big(\sum_{i=1}^{n}|A_i\cap A_{n+1}| - \sum_{1\le i_1<i_2\le n}|(A_{i_1}\cap A_{n+1})\cap(A_{i_2}\cap A_{n+1})| + \sum_{1\le i_1<i_2<i_3\le n}|(A_{i_1}\cap A_{n+1})\cap(A_{i_2}\cap A_{n+1})\cap(A_{i_3}\cap A_{n+1})| - \cdots + (-1)^{n-2}\sum_{1\le i_1<i_2<\cdots<i_{n-1}\le n}|(A_{i_1}\cap A_{n+1})\cap$

$$\cap(\mathrm{A}_{i_2}\cap\mathrm{A}_{n+1})\cap\cdots\cap(\mathrm{A}_{i_{n-1}}\cap\mathrm{A}_{n+1})|+(-1)^{n-1}|(\mathrm{A}_1\cap\mathrm{A}_{n+1})\cap(\mathrm{A}_2\cap\mathrm{A}_{n+1})\cap\cdots\cap(\mathrm{A}_n\cap(\mathrm{A}_{n+1})|\Big)=\sum_{i=1}^{n+1}|\mathrm{A}_i|-$$

$$-\Big(\sum_{1\le i_1<i_2\le n}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}|+\sum_{i=1}^{n}|\mathrm{A}_i\cap\mathrm{A}_{n+1}|\Big)+\Big(\sum_{1\le i_1<i_2<i_3\le n}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}\cap\mathrm{A}_{i_3}|+\sum_{1\le i_1<i_2\le n}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}\cap\mathrm{A}_{n+1}|\Big)-$$

$$-\cdots+(-1)^{n-1}\Big(|\mathrm{A}_1\cap\mathrm{A}_2\cap\cdots\cap\mathrm{A}_n|+\sum_{1\le i_1<i_2<\cdots<i_{n-1}\le n}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}\cap\cdots\cap\mathrm{A}_{i_{n-1}}\cap\mathrm{A}_{n+1}|\Big)+(-1)^n|\mathrm{A}_1\cap\mathrm{A}_2\cap$$

$$\cap\cdots\mathrm{A}_n\cap\mathrm{A}_{n+1}|=\sum_{i=1}^{n+1}|\mathrm{A}_i|-\sum_{1\le i_1<i_2\le n+1}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}|+\sum_{1\le i_1<i_2<i_3\le n+1}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}\cap\mathrm{A}_{i_3}|-\cdots+(-1)^n|\mathrm{A}_1\cap\mathrm{A}_2\cap$$

$\cap\cdots\cap\mathrm{A}_n\cap\mathrm{A}_{n+1}|$. ■

Πόρισμα Δ΄.6. (Αρχή του αποκλεισμού) Έστω $\mathrm{A}_1,\mathrm{A}_2,\ldots,\mathrm{A}_n$ υποσύνολα ενός βασικού συνόλου Ω με $|\Omega|=\mathrm{N}$. Τότε το πλήθος των στοιχείων του Ω που δεν ανήκουν σε κανένα από τα $\mathrm{A}_1,\mathrm{A}_2,\ldots,\mathrm{A}_n$ ισούται με

$$\mathrm{N}-\sum_{i=1}^{n}|\mathrm{A}_i|+\sum_{1\le i_1<i_2\le n}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}|-\sum_{1\le i_1<i_2<i_3\le n}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}\cap\mathrm{A}_{i_3}|+\cdots+$$
$$+(-1)^{n-1}\sum_{1\le i_1<i_2<\cdots<i_{n-1}\le n}|\mathrm{A}_{i_1}\cap\mathrm{A}_{i_2}\cap\cdots\cap\mathrm{A}_{i_{n-1}}|+(-1)^n|\mathrm{A}_1\cap\mathrm{A}_2\cap\cdots\cap\mathrm{A}_n|. \qquad (2)$$

Απόδειξη: Άμεση, με βάση το γεγονός ότι το πλήθος των στοιχείων που δεν ανήκουν σε κανένα από τα $\mathrm{A}_1,\mathrm{A}_2,\ldots,\mathrm{A}_n$ ισούται με $\mathrm{N}-|\mathrm{A}_1\cup\mathrm{A}_2\cup\cdots\cup\mathrm{A}_n|$. Το αποτέλεσμα προκύπτει αν εφαρμόσουμε τον τύπο (1) του προηγούμενου θεωρήματος. ■

Η Συνδυαστική αποτελεί έναν από τους πιο συναρπαστικούς κλάδους των Μαθηματικών. Μια πολύ καλή εισαγωγή στον κλάδο (κατά τη γνώμη μου-τα γούστα είναι προσωπικά) αποτελεί το βιβλίο των **CHEN Chuan-Chong** και **KOH Khee-Meng *"PRINCIPLES and TECHNIQUES in COMBINATORICS"*, World Scientific Publishing Co. Pte. Ltd., 1992.**