ΚΕΦΑΛΑΙΟ 2

Υπομνήσεις από τη Στοιχειώδη Θεωρία Αριθμών

Σκοπός τού παρόντος κεφαλαίου είναι η υπενθύμιση κάποιων αποτελεσμάτων τής Στοιχειώδους Θεωρίας Αριθμών, ορισμένα εκ των οποίων είναι ήδη γνωστά από το σχολείο[1] και θα χρησιμοποιηθούν κατ' επανάληψιν σε ό,τι θα ακολουθήσει. Μεταξύ αυτών συγκαταλέγονται η ταυτότητα τής ευκλειδείου διαιρέσεως, οι κύριες ιδιότητες και ο τρόπος υπολογισμού τού μεγίστου κοινού διαιρέτη και τού ελαχίστου κοινού πολλαπλασίου (δύο ή περισσότερων ακεραίων), η μονοσήμαντη παράσταση ενός φυσικού αριθμού ως γινομένου πρώτων αριθμών, το θεώρημα τού Euler περί ισοτιμίων και η περιγραφή των λύσεων γραμμικών ισοτιμιών.

2.1 ΔΙΑΙΡΕΣΗ ΑΚΕΡΑΙΩΝ

Η έννοια τής «διαιρέσεως» ήταν γνωστή και κατανοητή ήδη από αρχαιοτάτων χρόνων. Ο Ευκλείδης στο βιβλίο VII των «Στοιχείων» την περιγράφει με περισσή σαφήνεια (βασιζόμενος στη γεωμετρική-ανθυφαιρετική μέθοδο).

2.1.1 Ορισμός. Έστω ότι οι a, b είναι δυο ακέραιοι αριθμοί. Εάν υπάρχει ένας ακέραιος αριθμός c, τέτοιος ώστε να ισχύει η ισότητα $b = ac$, τότε λέμε ότι ο a **διαιρεί τον** b και ότι ο b **είναι διαιρετός** (ή **διαιρείται**) **διά τού** a ή -ισοδυνάμως- ότι ο b

[1] Πρβλ. Λ. Αδαμόπουλου, Β. Βισκαδουράκη, Δ. Γαβαλά, Γ. Πολύζου και Α. Σβέρκου: *Μαθηματικά* (Β′ Τάξη Ενιαίου Λυκείου, Θετική και Τεχνολογική Κατεύθυνση), ΟΕΔΒ, Αθήνα, 1998, κεφ. 4, σελ. 135-184.

είναι **πολλαπλάσιο τού** a και ότι ο a είναι **διαιρέτης** ή **παράγοντας** τού b. Όταν ο a διαιρεί τον b γράφουμε $a \mid b$, ενώ όταν ο a δεν διαιρεί τον b γράφουμε $a \nmid b$.

2.1.2 Παράδειγμα. Οι *άρτιοι* (και αντιστοίχως, οι *περιττοί*) ακέραιοι αριθμοί είναι εξ ορισμού εκείνοι οι ακέραιοι αριθμοί οι οποίοι διαιρούνται (και αντιστοίχως, δεν διαιρούνται) διά τού 2.

2.1.3 Πρόταση. (i) $a \mid 0$ *για κάθε* $a \in \mathbb{Z}$.

(ii) $\pm 1 \mid a$ *για κάθε* $a \in \mathbb{Z}$.

(iii) *Εάν* $0 \mid b$, *τότε* $b = 0$.

(iv) *Εάν* $b \mid \pm 1$, *τότε* $b = \pm 1$.

ΑΠΟΔΕΙΞΗ. (i) Προφανώς $0 = a \cdot 0$.

(ii) Επειδή $a = 1 \cdot a = (-1) \cdot (-a)$, έχουμε $\pm 1 \mid a$ για οιονδήποτε $a \in \mathbb{Z}$.

(iii) Εάν $0 \mid b$, τότε $b = 0 \cdot c$ για κάποιον $c \in \mathbb{Z}$, οπότε κατ' ανάγκην $b = 0$.

(iv) Εάν $b \mid \pm 1$, τότε $\pm 1 = b \cdot c$ για κάποιον $c \in \mathbb{Z}$, οπότε κατ' ανάγκην έχουμε $(b, c) \in \{(\pm 1, \pm 1), (\pm 1, \mp 1)\}$. □

2.1.4 Σημείωση. Σε ό,τι ακολουθεί σημειώνουμε ως $|a| = \text{sign}(a)\, a$ την *απόλυτη τιμή* ενός ακεραίου a (βλ. 1.8.30).

2.1.5 Πρόταση. *Εάν τα* $a, b, c, d \in \mathbb{Z}$,*τότε ισχύουν τα ακόλουθα*:

(i) $a \mid b \iff -a \mid b \iff a \mid -b \iff |a| \mid |b|$.

(ii) *Εάν* $a \mid b$ *και* $b \neq 0$, *τότε* $|a| \leq |b|$.

(iii) *Εάν* $a \mid b$ *και* $b \mid a$, *τότε* $|a| = |b|$.

(iv) *Εάν* $a \mid b$ *και* $c \mid d$, *τότε* $ac \mid bd$.

(v) *Εάν* $a \mid b$ *και* $b \mid c$, *τότε* $a \mid c$.

(vi) *Εάν*[2] $a \mid b$ *και* $a \mid c$, *τότε* $a \mid bx + cy$ *για κάθε* $x, y \in \mathbb{Z}$.

ΑΠΟΔΕΙΞΗ. (i) Προφανές επί τη βάσει τού ορισμού τής διαιρετότητας ακεραίων.

(ii) Εάν $a \mid b$ και $b \neq 0$, τότε υπάρχει μη μηδενικός ακέραιος a' με $b = aa'$. Επομένως, $|b| = |a|\,|a'|$, απ' όπου έπεται ότι $|a| \leq |b|$.

(iii) Εάν οι a και b είναι αμφότεροι μη μηδενικοί, τότε -λόγω τού (ii)- $|a| \leq |b|$ και $|a| \geq |b|$, οπότε $|a| = |b|$. Εάν $a = 0$, τότε από τη σχέση διαιρετότητας $a \mid b$ λαμβάνουμε $b = 0$ (βλ. 2.1.3 (iii)). Παρομοίως εάν $b = 0$, τότε από την $b \mid a$ λαμβάνουμε $a = 0$. Άρα σε κάθε περίπτωση $|a| = |b|$.

[2]Γενικότερα, εάν $n \in \mathbb{N}$, $b_1, \ldots, b_n \in \mathbb{Z}$, και $a \mid b_j$ για κάθε $j \in \{1, \ldots, n\}$, τότε (ακολουθώντας την ίδια συλλογιστική) έχουμε $a \mid \sum_{j=1}^{n} x_j b_j$ για οιουσδήποτε $x_1, \ldots, x_n \in \mathbb{Z}$.

(iv) Υποθέτοντας ότι $a \mid b$ και $c \mid d$, θα υπάρχουν ακέραιοι e, f, τέτοιοι ώστε να ισχύουν οι ισότητες $b = ae$ και $d = cf$. Κατά συνέπειαν,

$$bd = acef \Longrightarrow ac \mid bd.$$

(v) Υποθέτοντας ότι $a \mid b$ και $c \mid d$, θα υπάρχουν ακέραιοι e, f, τέτοιοι ώστε να ισχύουν οι ισότητες $b = ae$ και $c = bf$. Επομένως,

$$c = bf = aef \Longrightarrow a \mid c.$$

(vi) Εάν $a \mid b$ και $a \mid c$, θα υπάρχουν ακέραιοι e, f, τέτοιοι ώστε να ισχύουν οι ισότητες $b = ae$ και $c = af$. Συνεπώς,

$$bx + cy = aex + afy = a(ex + fy) \Longrightarrow a \mid bx + cy$$

για οιουσδήποτε $x, y \in \mathbb{Z}$. □

2.1.6 Θεώρημα. (Η ταυτότητα τής ευκλείδειας διαιρέσεως)
Εάν υποθέσουμε ότι $a \in \mathbb{Z}$ *και ότι* $b \in \mathbb{Z} \setminus \{0\}$, *τότε υπάρχει ένα* μονοσημάντως ορισμένο *ζεύγος* $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, *ούτως ώστε*

$$\boxed{a = qb + r, \text{ όπου } 0 \leq r < |b|\,.} \tag{2.1}$$

ΑΠΟΔΕΙΞΗ. Εν πρώτοις θα αποδείξουμε την *ύπαρξη* ενός τέτοιου ζεύγους ακεραίων (q, r). Θεωρούμε τα σύνολα

$$A := \{\, a - xb \mid x \in \mathbb{Z} \} \quad \text{και} \quad S := \{\, y \in A \mid y \geq 0 \}\,.$$

Το S δεν είναι κενό, διότι θέτοντας $x = -|a|\text{sign}(b)$ λαμβάνουμε

$$a - xb = a + |a|\,|b| \geq 0,$$

δεδομένου -εξ υποθέσεως- ότι $|b| \geq 1$. Ως εκ τούτου, το S διαθέτει ένα ελάχιστο στοιχείο $r \geq 0$ (βλ. πρόταση 1.7.27). Αυτό σημαίνει ότι $r = a - qb$ για κάποιον $q \in \mathbb{Z}$, οπότε $a = qb + r$. Υποθέτοντας ότι το r δεν ικανοποιεί την $r < |b|$, θα είχαμε

$$r \geq |b| > 0 \Longrightarrow 0 \leq r - |b| < r \Longrightarrow r - |b| = a - qb - |b| = a - (q + \text{sign}\,(b))b,$$

ήτοι ότι $r - |b| \in S$, κάτι το οποίο θα αντέφασκε προς την επιλογή τού r. Κατά συνέπειαν, οι ανισότητες $0 \leq r < |b|$ είναι όντως αληθείς. Απομένει λοιπόν να δείξουμε ότι το ανωτέρω ζεύγος (q, r) που ικανοποιεί την (2.1) είναι, επιπροσθέτως, και *μονοσημάντως ορισμένο*. Ας υποθέσουμε ότι

$$a = qb + r = q'b + r',$$

όπου $(q', r') \in \mathbb{Z} \times \mathbb{Z}$, και ότι $0 \leq r, r' < |b|$. Τότε

$$\left.\begin{array}{c} |r - r'| = |b|\,|q - q'| \\ \text{και} \\ 0 \leq |r - r'| < |b| \end{array}\right\} \Longrightarrow |b|\,|q - q'| < |b| \Longrightarrow |q - q'| < 1 \underset{q,q' \in \mathbb{Z}}{\Longrightarrow} q = q'.$$

Άρα $r = a - qb = a - q'b = r'$, δηλαδή κατ' ανάγκην $(q, r) = (q', r')$. □

2.1.7 Ορισμός. Τα q και r τής ταυτότητας (2.1) ονομάζονται το **πηλίκο** και, αντιστοίχως, το **υπόλοιπο** τής διαιρέσεως τού a διά τού b.

2.2 ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ ΚΑΙ ΕΛΑΧΙΣΤΟ ΚΟΙΝΟ ΠΟΛΛΑΠΛΑΣΙΟ

2.2.1 Ορισμός. Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν οι $a_1, \ldots, a_n$ είναι ακέραιοι αριθμοί, με έναν τουλάχιστον εξ αυτών $\neq 0$, τότε οιοσδήποτε ακέραιος που διαιρεί καθέναν εκ των $a_1, \ldots, a_n$ καλείται **κοινός διαιρέτης** των $a_1, \ldots, a_n$. Έστω S το σύνολο των θετικών κοινών διαιρετών των $a_1, \ldots, a_n$. Προφανώς το S είναι μη κενό, καθότι $1 \in S$. Επειδή $a_k \neq 0$ για κάποιον $k \in \{1, ..., n\}$, έχουμε $\delta \mid a_k$ και, ως εκ τούτου, $\delta \leq |a_k|$, για οιοδήποτε στοιχείο δ τού S. Κατά συνέπειαν, το S είναι πεπερασμένο. Το μέγιστο στοιχείο τού συνόλου S (ως προς την " $\leq$ ") καλείται **μέγιστος κοινός διαιρέτης (=: μκδ)** των $a_1, \ldots, a_n$ και συμβολίζεται ως μκδ$(a_1, \ldots, a_n)$. Σημειωτέον ότι για κάθε $a \in \mathbb{Z}$ το σύνολο των θετικών διαιρετών τού a συμπίπτει με το σύνολο των θετικών διαιρετών τού $-a$. Επομένως,

$$\text{μκδ}(a_1, \ldots, a_n) = \text{μκδ}(|a_1|, \ldots, |a_n|),$$

δηλαδή ο μκδ των $a_1, \ldots, a_n$ είναι *ανεξάρτητος* των προσήμων τους. Επίσης, επειδή κάθε ακέραιος διαιρεί το μηδέν, έχουμε

$$\text{μκδ}(0, a_1, \ldots, a_n) = \text{μκδ}(a_1, \ldots, a_n).$$

(Γι' αυτόν τον λόγο μπορούμε εφεξής να υποθέτουμε ότι κανείς εκ των εκάστοτε θεωρουμένων ακεραίων $a_1, \ldots, a_n$ δεν είναι μηδέν.)

2.2.2 Ορισμός. Δυο μη αρνητικοί ακέραιοι a, b καλούνται **σχετικώς πρώτοι** όταν μκδ$(a, b) = 1$. (Επίσης, εναλλακτικώς, σε αυτήν την περίπτωση, λέμε ότι ο a είναι **πρώτος προς τον** b ή -ισοδυνάμως- ότι ο b είναι **πρώτος προς τον** a).

2.2.3 Ορισμός. Εάν $n \in \mathbb{N}$, $n \geq 2$, οι $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι αριθμοί και μκδ$(a_1, \ldots, a_n) = 1$, τότε λέμε ότι οι ακέραιοι $a_1, \ldots, a_n$ είναι **σχετικώς πρώτοι** ή

ότι είναι **πρώτοι μεταξύ τους**. Εάν μκδ$(a_j, a_k) = 1$ για οιουσδήποτε $j, k \in \{1, ..., n\}$ με $j \neq k$, τότε λέμε ότι οι ακέραιοι $a_1, \dots, a_n$ είναι **σχετικώς πρώτοι ανά δύο** (ή **ανά ζεύγη**) ή, εναλλακτικώς, ότι είναι **πρώτοι μεταξύ τους ανά δύο** (ή **ανά ζεύγη**).

2.2.4 Παρατήρηση. Εάν οι ακέραιοι $a_1, \dots, a_n$ είναι σχετικώς πρώτοι ανά δύο, τότε είναι και σχετικώς πρώτοι (ως ολότητα). Αντιθέτως, το να είναι οι ακέραιοι $a_1, \dots, a_n$ σχετικώς πρώτοι δεν σημαίνει ότι αυτοί είναι κατ' ανάγκην και σχετικώς πρώτοι ανά δύο. Π.χ., μκδ$(5, 6, 10) = 1$, με μκδ$(5, 6) = 1$, αλλά μκδ$(5, 10) = 5$ και μκδ$(6, 10) = 2$.

2.2.5 Θεώρημα. *Εάν $n \in \mathbb{N},\ n \geq 2$, οι $a_1, \dots, a_n$ μη μηδενικοί ακέραιοι και*

$$d = \text{μκδ}(a_1, \dots, a_n),$$

τότε υπάρχουν ακέραιοι αριθμοί $k_1, \dots, k_n$, τέτοιοι ώστε να ισχύει η ισότητα[3]

$$\boxed{d = k_1 a_1 + \cdots + k_n a_n.} \tag{2.2}$$

ΑΠΟΔΕΙΞΗ. Θεωρούμε το σύνολο

$$S := \left\{ \sum_{j=1}^{n} \lambda_j a_j \;\middle|\; \lambda_1, \dots, \lambda_n \in \mathbb{Z} \right\}.$$

Θέτοντας

$$\varepsilon_{j,l} := \begin{cases} 1, & \text{όταν } j = l, \\ 0, & \text{όταν } j \neq l, \end{cases}$$

για κάθε $j, l \in \{1, \dots, n\}$, έχουμε προφανώς

$$a_l = \sum_{j=1}^{n} \varepsilon_{j,l} a_j \in S,\ \ \forall l \in \{1, \dots, n\}.$$

Εάν κάποιος εκ των $a_1, \dots, a_n$ είναι > 0, τότε $S \cap \mathbb{N} \neq \varnothing$. Ωστόσο, το ότι $S \cap \mathbb{N} \neq \varnothing$ είναι *πάντοτε* αληθές, διότι ακόμη και εάν $a_l < 0$ για *κάθε* $l \in \{1, \dots, n\}$, έχουμε

$$-a_l = \sum_{j=1}^{n} (-\varepsilon_{j,l})\, a_j \in S \cap \mathbb{N}.$$

Ως εκ τούτου, το $S \cap \mathbb{N}$ διαθέτει *ελάχιστο* στοιχείο (βλ. πρόταση 1.7.27), ας πούμε το $d' = \sum_{j=1}^{n} k_j a_j$. Θα αποδείξουμε ότι $d' = d$. Πράγματι· για οιοδήποτε στοιχείο $m = \sum_{j=1}^{n} \lambda_j a_j$ τού S υπάρχει (κατά το θεώρημα 2.1.6) ένα μονοσημάντως ορισμένο ζεύγος $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, ούτως ώστε να ισχύει

$$m = qd' + r, \text{ όπου } 0 \leq r < d'.$$

[3] Είθισται να λέμε ότι μέσω τής (2.2) ο d εκφράζεται ως *ακέραιος γραμμικός συνδυασμός* των $a_1, \dots, a_n$ (με *συντελεστές* του τους $k_1, \dots, k_n$).

Υποθέτοντας ότι $r > 0$ καταλήγουμε σε κάτι το άτοπο, καθόσον

$$d' > r = \sum_{j=1}^{n} (\lambda_j - k_j q)\, a_j \in S.$$

Άρα $r = 0 \Longrightarrow d' \mid m$ και, ειδικότερα, $d' \mid a_j$ για κάθε $j \in \{1, \dots, n\}$. Επιπροσθέτως, για οιονδήποτε $\delta \in \mathbb{N}$, για τον οποίο ισχύει $\delta \mid a_1, \dots, \delta \mid a_n$, έχουμε

$$[\delta \mid k_1 a_1, \dots, \delta \mid k_n a_n] \Longrightarrow \delta \mid d' \Longrightarrow \delta \leq d'$$

(βλ. 2.1.5 (vi) και (ii)), οπότε τελικώς $d' = d$. □

2.2.6 Πόρισμα. *Εάν $n \in \mathbb{N},\ n \geq 2$, και οι $a_1, \dots, a_n$ είναι μη μηδενικοί ακέραιοι, τότε ένας θετικός ακέραιος d ισούται με τον* μκδ$(a_1, \dots, a_n)$ *εάν και μόνον εάν ισχύουν τα ακόλουθα*:

(i) $d \mid a_1, \dots, d \mid a_n$,

(ii) *για οιονδήποτε $\delta \in \mathbb{N}$, για τον οποίο ισχύει $\delta \mid a_1, \dots, \delta \mid a_n$, έχουμε $\delta \mid d$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το θεώρημα 2.2.5 υπάρχουν ακέραιοι $k_1, \dots, k_n$, τέτοιοι ώστε να ισχύει η ισότητα

$$\text{μκδ}(a_1, \dots, a_n) = k_1 a_1 + \cdots + k_n a_n.$$

Το (i) ισχύει εξ ορισμού. Για την απόδειξη τού (ii) αρκεί να θεωρήσουμε τυχόντα θετικό κοινό διαιρέτη δ των $a_1, \dots, a_n$ και να αποδείξουμε ότι αυτός διαιρεί τον μέγιστο κοινό διαιρέτη τους. Επειδή

$$\delta \mid a_j \Longrightarrow \delta \mid k_j a_j,\ \forall j \in \{1, \dots, n\},$$

διαπιστώνουμε πράγματι ότι $\delta \mid$μκδ$(a_1, \dots, a_n)$ (πρβλ. 2.1.5 (vi)). Και αντιστρόφως· εάν υποθέσουμε ότι ο d είναι ένας θετικός ακέραιος ο οποίος ικανοποιεί τα (i) και (ii), τότε ο d είναι κοινός διαιρέτης των $a_1, \dots, a_n$ (λόγω τού (i)) και *οισδήποτε* θετικός κοινός διαιρέτης δ των $a_1, \dots, a_n$ διαιρεί τον d (λόγω τού (ii)), οπότε $\delta \leq d$ (βλ. 2.1.5 (ii)). Επομένως, $d =$ μκδ$(a_1, \dots, a_n)$. □

2.2.7 Πόρισμα. *Έστω ότι $n \in \mathbb{N},\ n \geq 2$, και ότι οι $a_1, \dots, a_n$ είναι μη μηδενικοί ακέραιοι. Εάν ο d είναι ένας θετικός κοινός διαιρέτης των $a_1, \dots, a_n$, ο οποίος γράφεται υπό τη μορφή $d = k_1 a_1 + \cdots + k_n a_n$, με τους $k_1, \dots, k_n$ ακεραίους, τότε έχουμε $d =$* μκδ$(a_1, \dots, a_n)$.

ΑΠΟΔΕΙΞΗ. Έστω δ ένας θετικός κοινός διαιρέτης των $a_1, \dots, a_n$. Επειδή

$$\delta \mid a_j \Longrightarrow \delta \mid k_j a_j,\ \forall j \in \{1, \dots, n\},$$

έχουμε $\delta \mid d$ (βλ. 2.1.5 (vi)). Κατά συνέπειαν, $d =$ μκδ$(a_1, \dots, a_n)$ βάσει τού πορίσματος 2.2.7. □

2.2.8 Πόρισμα. *Εάν* $n \in \mathbb{N},\ n \geq 2$, *και οι* $a_1, \ldots, a_n$ *είναι μη μηδενικοί ακέραιοι, τότε οι* $a_1, \ldots, a_n$ *είναι πρώτοι μεταξύ τους εάν και μόνον εάν υπάρχουν ακέραιοι αριθμοί* $k_1, \ldots, k_n$, *τέτοιοι ώστε να ισχύει η ισότητα*

$$\boxed{k_1a_1 + \cdots + k_na_n = 1.}$$

ΑΠΟΔΕΙΞΗ. Εάν οι $a_1, \ldots, a_n$ είναι πρώτοι μεταξύ τους, τότε η ως άνω ισότητα είναι προφανής από το θεώρημα 2.2.5. Εάν, αντιστρόφως, $k_1a_1 + \cdots + k_na_n = 1$ για κάποιους ακεραίους $k_1, \ldots, k_n$, έχουμε $1 \mid a_j$ για κάθε $j \in \{1, \ldots, n\}$, οπότε μκδ$(a_1, \ldots, a_n) = 1$ δυνάμει τού πορίσματος 2.2.7. □

2.2.9 Πόρισμα. *Εάν* $a, m, n \in \mathbb{Z}\setminus\{0\}$, *τότε* μκδ$(a, mn) = 1$ *εάν και μόνον εάν* μκδ$(a, m) = 1$ *και* μκδ$(a, n) = 1$.

ΑΠΟΔΕΙΞΗ. Εάν μκδ$(a, mn) = 1$, τότε κατά το πόρισμα 2.2.8 υπάρχουν $k, l \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα $ka+lmn = 1$. Με εκ νέου εφαρμογή τού πορίσματος 2.2.8 (και, συγκεκριμένα, τής αντίστροφης συνεπαγωγής που δηλοί το «μόνον εάν») συμπεραίνουμε ότι μκδ$(a, m) = 1$ και μκδ$(a, n) = 1$. Και αντιστρόφως· υποθέτοντας ότι μκδ$(a, m) = 1$ και μκδ$(a, n) = 1$, θα υπάρχουν $r, s, t, u \in \mathbb{Z}$, τέτοιοι ώστε

$$\left.\begin{array}{r} ra + sm = 1 \\ ta + un = 1 \end{array}\right\} \Longrightarrow ra + sm\,(ta + un) = 1 = (r + stm)\,a + (su)mn,$$

οπότε και πάλι μέσω τού 2.2.8 προκύπτει ότι μκδ$(a, mn) = 1$. □

2.2.10 Πόρισμα. *Εάν* $a, b, c \in \mathbb{Z}\setminus\{0\}$, μκδ$(a, b) = 1$ *και* $a \mid bc$, *τότε* $a \mid c$.

ΑΠΟΔΕΙΞΗ. Επειδή μκδ$(a, b) = 1$, βάσει τού 2.2.8 υπάρχουν $k, l \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα $ka + lb = 1$. Ως εκ τούτου,

$$kac + lbc = c,$$

και επειδή $a \mid ac$ και $a \mid bc$, έχουμε $a \mid c$. □

2.2.11 Πρόταση. *Εάν* $n \in \mathbb{N},\ n \geq 2$, *και εάν οι* $\lambda, a_1, \ldots, a_n$ *είναι μη μηδενικοί ακέραιοι,τότε ισχύουν τα ακόλουθα*:

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

(ii) *εάν* μκδ$(a_1, \ldots, a_n) = d$, *τότε* μκδ$(\frac{a_1}{d}, \ldots, \frac{a_n}{d}) = 1$, *και*

(iii) μκδ$(a_1, \ldots, a_n)$ = μκδ$(a_1 + \nu_2a_2 + \cdots + \nu_na_n, a_2, ..., a_n)$, *για οιουσδήποτε* $\nu_2, .., \nu_n \in \mathbb{Z}$.

ΑΠΟΔΕΙΞΗ. (i) Εάν μκδ$(a_1, \dots, a_n) = d$, τότε κατά το θεώρημα 2.2.5 υπάρχουν ακέραιοι $k_1, \dots, k_n$, τέτοιοι ώστε να ισχύει η ισότητα $d = k_1a_1 + \cdots + k_na_n$. Επομένως,

$$d\,|\lambda| = \sum_{j=1}^{n} k_j a_j\,|\lambda| = \sum_{j=1}^{n} (\text{sign}\,(\lambda)\,k_j)\;\; a_j\lambda,$$

κι επειδή $d \mid a_j \Longrightarrow d\,|\lambda| \mid a_j\lambda$, για κάθε $j \in \{1, \dots, n\}$, ο μκδ των $\lambda a_1, \dots, \lambda a_n$ είναι ο $d\,|\lambda|$ δυνάμει τού πορίσματος 2.2.7.

(ii) Σύμφωνα με το (i) έχουμε

$$d = \text{μκδ}(a_1, \dots, a_n) = \text{μκδ}(d\,\tfrac{a_1}{d}, \dots, d\,\tfrac{a_n}{d}) = d\;\text{μκδ}(\tfrac{a_1}{d}, \dots, \tfrac{a_n}{d}),$$

οπότε μκδ$(\frac{a_1}{d}, \dots, \frac{a_n}{d}) = 1$.

(iii) Κατόπιν εισαγωγής των συντομογραφιών

$$\text{μκδ}(a_1, \dots, a_n) =: d, \qquad \text{μκδ}(a_1 + \nu_2a_2 + \cdots + \nu_na_n, a_2, ..., a_n) =: d',$$

παρατηρούμε ότι

$$[d \mid a_j \Longrightarrow d \mid \nu_ja_j,\ \forall j \in \{2, \dots, n\}] \Longrightarrow d \mid a_1 + \nu_2a_2 + \cdots + \nu_na_n.$$

Κατά το πόρισμα 2.2.6, $d \mid d'$. Και αντιστρόφως· επειδή

$$d' \mid a_1 + \nu_2a_2 + \cdots + \nu_na_n \;\;\text{και}\;\; [d' \mid a_j \Longrightarrow d' \mid \nu_ja_j,\ \forall j \in \{2, \dots, n\}]\,,$$

έχουμε

$$d' \mid a_1 + \nu_2a_2 + \cdots + \nu_na_n - (\nu_2a_2 + \cdots + \nu_na_n),$$

ήτοι $d' \mid a_1$, οπότε $d' \mid a_j,\ \forall j \in \{1, 2, \dots, n\}$, απ' όπου έπεται ότι $d' \mid d$ (βλ. 2.2.6). Επειδή οι d και d' είναι θετικοί ακέραιοι, οι σχέσεις διαιρετότητας $d \mid d'$ και $d' \mid d$ μας οδηγούν στην ισότητα $d = d'$ (βλ. 2.1.5 (iii)). □

2.2.12 Πρόταση. *Εάν $n \in \mathbb{N},\ n \geq 3$, και εάν οι $a_1, \dots, a_n$ είναι μη μηδενικοί ακέραιοι, τότε για κάθε $k \in \mathbb{Z}, 1 \leq k \leq n-2$, ισχύει η ισότητα*

$$\boxed{\text{μκδ}(a_1, \dots, a_n) = \text{μκδ}(a_1, \dots, a_k,\ \text{μκδ}(a_{k+1}, \dots, a_n)).} \qquad (2.3)$$

ΑΠΟΔΕΙΞΗ. Επειδή μκδ$(a_1, \dots, a_n) \mid a_j$ για κάθε $j \in \{k+1, \dots, n\}$ έχουμε

$$\text{μκδ}(a_1, \dots, a_n) \mid \text{μκδ}(a_{k+1}, \dots, a_n).$$

Επομένως, $\mu\kappa\delta(a_1,\dots,a_n) \mid a_j$ για οιονδήποτε δείκτη $j \in \{1,\dots,n\}$ και $\mu\kappa\delta(a_1,\dots,a_n) \mid \mu\kappa\delta(a_{k+1},\dots,a_n)$, απ' όπου συνάγουμε ότι

$$\mu\kappa\delta(a_1,\dots,a_n) \mid \mu\kappa\delta(a_1,\dots,a_k,\mu\kappa\delta(a_{k+1},\dots,a_n)). \tag{2.4}$$

Και αντιστρόφως· $\mu\kappa\delta(a_1,\dots,a_k,\mu\kappa\delta(a_{k+1},\dots,a_n)) \mid a_j$ για κάθε $j \in \{1,\dots,k\}$ και

$$\mu\kappa\delta(a_1,\dots,a_k,\mu\kappa\delta(a_{k+1},\dots,a_n)) \mid \mu\kappa\delta(a_{k+1},\dots,a_n),$$

οπότε $\mu\kappa\delta(a_1,\dots,a_k,\mu\kappa\delta(a_{k+1},\dots,a_n)) \mid a_j$ για κάθε $j \in \{1,\dots,n\}$, που σημαίνει ότι

$$\mu\kappa\delta(a_1,\dots,a_k,\mu\kappa\delta(a_{k+1},\dots,a_n)) \mid \mu\kappa\delta(a_1,\dots,a_n). \tag{2.5}$$

Επειδή οι προκείμενοι μέγιστοι κοινοί διαιρέτες είναι θετικοί ακέραιοι, από τις (2.4), (2.5) και το (iii) τής προτάσεως 2.1.5 συμπεραίνουμε την ισχύ τής ισότητας (2.3). □

2.2.13 Παρατήρηση. Θέτοντας $k=1$ και εφαρμόζοντας τον τύπο (2.3) $n-1$ φορές είναι δυνατή η αναγωγή τής ευρέσεως τού μεγίστου κοινού διαιρέτη $n \geq 3$ μη μηδενικών ακεραίων αριθμών $a_1,\dots,a_n$ στην εύρεση τού μεγίστου κοινού διαιρέτη $n-1$ *ζευγών* μη μηδενικών ακεραίων.

► **Ευκλείδειος αλγόριθμος προσδιορισμού μκδ**. Ο υπολογισμός τού μεγίστου κοινού διαιρέτη *δύο* τυχόντων μη μηδενικών ακεραίων $r_0 = a$, $r_1 = b$ μπορεί να εκτελεσθεί με τη βοήθεια τού λεγομένου *Ευκλειδείου αλγορίθμου*, ο οποίος βασίζεται στη χρήση πεπερασμένου πλήθους ταυτοτήτων τής Ευκλειδείου διαιρέσεως (2.1) ως ακολούθως: Επειδή $\mu\kappa\delta(a,b) = \mu\kappa\delta(|a|,|b|)$ μπορούμε -χωρίς βλάβη τής γενικότητας- να υποθέσουμε ότι $a \geq b > 0$. Κατά το θεώρημα 2.1.6 υπάρχουν μονοσημάντως ορισμένα ζεύγη ακεραίων αριθμών (q_j, r_j), $1 \leq j \leq n+1$, ούτως ώστε να ισχύουν οι ισότητες:

$$\begin{cases} r_0 = r_1 q_1 + r_2, & 0 \leq r_2 < r_1 \\ r_1 = r_2 q_2 + r_3, & 0 \leq r_3 < r_2 \\ r_2 = r_3 q_3 + r_4, & 0 \leq r_4 < r_3 \\ \cdots\cdots & \cdots\cdots \\ r_{n-3} = r_{n-2} q_{n-2} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} = r_n q_n + r_{n+1}, & 0 \leq r_{n+1} < r_n. \end{cases} \tag{2.6}$$

(Εάν $\exists r_j$, $j \geq 2$, με $r_j = 0$, τότε σταματούμε). Εξ αυτών συνάγουμε -ιδιαιτέρως- ότι

$$0 \leq r_{n+1} < r_n < r_{n-1} < \cdots < r_3 < r_2 < r_1 \leq r_0.$$

Εάν υποθέταμε ότι για *κάθε* φυσικό αριθμό n το υπόλοιπο r_{n+1} είναι $\neq 0$, θα καταλήγαμε στο συμπέρασμα ότι μεταξύ τού 0 και τού $r_0 = a$ υπάρχουν *άπειροι* (διακεκριμένοι) φυσικοί αριθμοί, κάτι που θα ήταν άτοπο. Ως εκ τούτου, υπάρχει (κατ' ανάγκην) κάποιος φυσικός αριθμός, ας τον πούμε n_*, για τον οποίο $r_{n_*} \neq 0$ και $r_{n_*+1} = 0$.

2.2.14 Πρόταση. (Ευκλείδειος αλγόριθμος) *Ο μέγιστος κοινός διαιρέτης των a και b είναι ο*

$$\boxed{\text{μκδ}(a, b) = r_{n_*}.} \tag{2.7}$$

ΑΠΟΔΕΙΞΗ. Σύμφωνα με την πρόταση 2.2.11 (iii) έχουμε

$$\text{μκδ}(a, b) = \text{μκδ}(r_0, r_1) = \text{μκδ}(r_1, r_0) = \text{μκδ}(r_1, r_1 q_1 + r_2) = \text{μκδ}(r_1, r_2)$$

και, κατ' αναλογίαν,

$$\text{μκδ}(r_1, r_2) = \text{μκδ}(r_2, r_3) = \cdots = \text{μκδ}(r_{n_*-1}, r_{n_*}) = \text{μκδ}(r_{n_*} q_{n_*}, r_{n_*}) = r_{n_*},$$

απ' όπου έπεται η ισότητα (2.7). □

2.2.15 Παράδειγμα. Ο μέγιστος κοινός διαιρέτης των $a = 240$ και $b = 50$, λαμβανομένου υπ' όψιν ότι

$$\begin{cases} 240 = 50 \cdot 4 + 40, \\ 50 = 40 \cdot 1 + 10, \\ 40 = 10 \cdot 4 + 0, \end{cases}$$

υπολογίζεται μέσω των ισοτήτων $\text{μκδ}(240, 50) = \text{μκδ}(50, 40) = \text{μκδ}(40, 10) = 10$.

2.2.16 Σημείωση. Το θεώρημα 2.2.5 μας πληροφορεί ότι ο μέγιστος κοινός διαιρέτης $n \geq 2$ μη μηδενικών ακεραίων αριθμών εκφράζεται ως ακέραιος γραμμικός συνδυασμός αυτών των αριθμών. Ωστόσο, εξαιτίας τής καθαρώς «υπαρξιακής» αποδείξεώς του, δεν μας παρέχει καμία πληροφορία για τον τρόπο *υπολογισμού* των συντελεστών τού εν λόγω γραμμικού συνδυασμού. Αντιθέτως, όταν $n = 2$, ο Ευκλείδειος αλγόριθμος μας διασφαλίζει κατά τρόπο *κατασκευαστικό* ένα *φυσικό ζεύγος* ακεραίων, οι οποίοι παίζουν τον ρόλο συντελεστών τού $\text{μκδ}(a, b)$ ως ακεραίου γραμμικού συνδυασμού των a και b, ως ακολούθως:

2.2.17 Πρόταση. *Εάν οι a και b είναι δυο θετικοί ακέραιοι αριθμοί και $a \geq b$, τότε*

$$\boxed{\text{μκδ}(a, b) = s_{n_*} a + t_{n_*} b,} \tag{2.8}$$

με[4]

$$\begin{cases} s_0 = 1, & t_0 = 0, \\ s_1 = 0, & t_1 = 1, \\ s_j = s_{j-2} - q_{j-1}s_{j-1}, & t_j = t_{j-2} - q_{j-1}t_{j-1}, \end{cases}$$

για κάθε $j \in \{2, \dots, n_*\}$, *όπου τα* $q_1, q_2, \dots, q_{n_*-1}$ *είναι τα πηλίκα των διαιρέσεων* (2.6) *των εμφανιζομένων κατά την εκτέλεση τού Ευκλειδείου αλγορίθμου για τον προσδιορισμό τού* μκδ(a, b) *και* n_* *ο ληκτικός του φυσικός αριθμός (για τον οποίο* $r_{n_*} \neq 0$ *και* $r_{n_*+1} = 0$*).*

ΑΠΟΔΕΙΞΗ. Χρησιμοποιώντας τις διαιρέσεις (2.6) θα αποδείξουμε τις ισότητες

$$r_j = s_j a + t_j b, \ \ \forall j \in \{0, 1, \dots, n_*\}, \tag{2.9}$$

απ' όπου προκύπτει η (2.8), λόγω τού ότι μκδ$(a, b) = r_{n_*}$. Προς τούτο αρκεί να εργασθούμε επαγωγικώς επί τού j. Για $j = 0$ έχουμε

$$a = r_0 = 1 \cdot a + 0 \cdot b = s_0 a + t_0 b,$$

ενώ για $j = 1$,

$$b = r_1 = 0 \cdot a + 1 \cdot b = s_1 a + t_1 b.$$

Υποθέτοντας ότι $r_j = s_j a + t_j b$ για κάθε $j \in \{1, \dots, k-1\}$, όπου $1 \leq k \leq n_*$, έχουμε

$$r_k = r_{k-2} - r_{k-1}q_{k-1},$$

οπότε, λόγω τής επαγωγικής υποθέσεώς μας,

$$\begin{aligned} r_k &= (s_{k-2}a + t_{k-2}b) - (s_{k-1}a + t_{k-1}b)\, q_{k-1} \\ &= (s_{k-2} - s_k q_{k-1})\, a + (t_{k-2} - t_{k-1}q_{k-1})\, b \\ &= s_k a + t_k b, \end{aligned}$$

απ' όπου έπεται το ζητούμενο. □

2.2.18 Παρατήρηση. (i) Χρησιμοποιώντας $n - 1$ φορές την (2.3) (για $k = 1$, βλ. παρατήρηση 2.2.13) και την ισότητα (2.8) είναι δυνατός ο υπολογισμός *συγκεκριμένων* συντελεστών $k_1, \dots, k_n \in \mathbb{Z}$ τού $d =$ μκδ$(a_1, \dots, a_n)$ για την έκφρασή του ως γραμμικού συνδυασμού (2.2). Ωστόσο, θα πρέπει εδώ να τονισθεί ότι η επιλογή

[4] Για τον συσχετισμό αυτών των πεπερασμένων ακολουθιών με την κατά αρκετά κομψό τρόπο παράσταση τού πηλίκου τού $\frac{a}{b} = \frac{a/\text{μκδ}(a,b)}{b/\text{μκδ}(a,b)}$ ως *πεπερασμένου συνεχούς κλάσματος* πρβλ. D. Burton: *Elementary Number Theory*, third ed., McGraw-Hill Co., 1997, εν. 14.2, σελ. 290.

ακεραίων $k_1, \ldots, k_n$, τέτοιων ώστε να ισχύει η (2.2) δεν είναι κατά κανέναν τρόπο μονοσημάντως ορισμένη!

(ii) Για να καταστεί περισσότερο σαφές το ότι η επιλογή των ως άνω ακεραίων συντελεστών δεν είναι μονοσημάντως ορισμένη *ακόμη και για* $n = 2$, θεωρούμε δυο μη μηδενικούς ακεραίους a και b και θέτουμε $d = \text{μκδ}(a, b)$. Εάν

$$d = sa + tb,$$

για κατάλληλους $s, t \in \mathbb{Z}$, τότε

$$d = \left(s + k\left(\frac{b}{d}\right)\right)a + \left(t - k\left(\frac{a}{d}\right)\right)b,$$

για *οιονδήποτε* $k \in \mathbb{Z}$.

2.2.19 Ορισμός. Έστω ότι $n \in \mathbb{N}$ και ότι οι $a_1, \ldots, a_n$ είναι ακέραιοι αριθμοί. Ένας ακέραιος μ καλείται **κοινό πολλαπλάσιο** των $a_1, .., a_n$ όταν $a_1 \mid \mu, .., a_n \mid \mu$. (Σημειωτέον ότι εάν ένας εκ των $a_1, \ldots, a_n$ είναι ίσος με το 0, τότε το μοναδικό πολλαπλάσιό τους είναι το 0).

2.2.20 Ορισμός. Έστω ότι $n \in \mathbb{N}$ και ότι οι $a_1, \ldots, a_n$ είναι μη μηδενικοί ακέραιοι αριθμοί. Προφανώς ο φυσικός αριθμός $|a_1 \cdots a_n|$ είναι ένα κοινό πολλαπλάσιο των $a_1, \ldots, a_n$. Ως εκ τούτου, το σύνολο των θετικών πολλαπλασίων των $a_1, \ldots, a_n$ είναι μη κενό και διαθέτει ένα *ελάχιστο* στοιχείο. Το στοιχείο αυτό καλείται **ελάχιστο κοινό πολλαπλάσιο (=: εκπ)** των $a_1, \ldots, a_n$ και συμβολίζεται ως εκπ$(a_1, \ldots, a_n)$. Επειδή το σύνολο των θετικών πολλαπλασίων των $a_1, \ldots, a_n$ ισούται με το σύνολο των θετικών πολλαπλασίων των $|a_1|, \ldots, |a_n|$, συμπεραίνουμε ότι εκπ$(a_1, \ldots, a_n) =$ εκπ$(|a_1|, \ldots, |a_n|)$.

2.2.21 Πρόταση. *Εάν* $n \in \mathbb{N}$ *και οι* $a_1, \ldots, a_n$ *είναι μη μηδενικοί ακέραιοι, τότε ένας θετικός ακέραιος* m *ισούται με το* εκπ$(a_1, \ldots, a_n)$ *εάν και μόνον εάν ισχύουν τα ακόλουθα*:

(i) $a_1 \mid m, \ldots, a_n \mid m$,

(ii) *για οιονδήποτε θετικό ακέραιο* μ, *για τον οποίο ισχύει* $a_1 \mid \mu, \ldots, a_n \mid \mu$, *έχουμε* $m \mid \mu$.

ΑΠΟΔΕΙΞΗ. Εάν $m =$ εκπ$(a_1, \ldots, a_n)$, τότε εξ ορισμού $a_1 \mid m, \ldots, a_n \mid m$, οπότε ισχύει το (i). Εξάλλου, για οιονδήποτε θετικό ακέραιο μ, για τον οποίο ισχύει $a_1 \mid \mu, \ldots, a_n \mid \mu$, υπάρχει (κατά το 2.1.6) ένα μονοσημάντως ορισμένο ζεύγος $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, ούτως ώστε να ισχύει

$$\mu = qm + r, \text{ όπου } 0 \leq r < m.$$

Επειδή

$$\left.\begin{array}{r} a_1 \mid m, \ldots, a_n \mid m \\ a_1 \mid \mu, \ldots, a_n \mid \mu \end{array}\right\} \Longrightarrow a_1 \mid r, \ldots, a_n \mid r,$$

το r είναι ένα κοινό πολλαπλάσιο των $a_1, \ldots, a_n$. Άρα $r = 0$ (διότι εάν $r > 0$, θα είχαμε $r \geq m$, ήτοι κάτι το άτοπο), οπότε ισχύει και το (ii).

Και αντιστρόφως· υποθέτοντας την ισχύ των ιδιοτήτων (i) και (ii) για έναν θετικό ακέραιο m, το m είναι ένα κοινό πολλαπλάσιο των $a_1, \ldots, a_n$ και για οιοδήποτε κοινό πολλαπλάσιο μ των $a_1, \ldots, a_n$ έχουμε $m \mid \mu$, απ' όπου συμπεραίνουμε ότι $m \leq \mu$, ήτοι ότι $m = \text{εκπ}(a_1, \ldots, a_n)$. □

2.2.22 Πρόταση. *Εάν $n \in \mathbb{N}$ και εάν οι $\lambda, a_1, \ldots, a_n$ είναι μη μηδενικοί ακέραιοι,τότε ισχύουν τα ακόλουθα*:

(i) $\text{εκπ}(\lambda a_1, \ldots, \lambda a_n) = |\lambda|\ \text{εκπ}(a_1, \ldots, a_n)$,

(ii) *εάν* $\text{εκπ}(a_1, \ldots, a_n) = m$, *τότε* $\text{μκδ}(\frac{m}{a_1}, \ldots, \frac{m}{a_n}) = 1$.

ΑΠΟΔΕΙΞΗ. (i) Εάν $\text{εκπ}(a_1, \ldots, a_n) = m$, τότε για κάθε $j \in \{1, \ldots, n\}$

$$a_j \mid m \Longrightarrow \lambda a_j \mid |\lambda|\, m,$$

οπότε, δυνάμει τής προτάσεως 2.2.21, $\text{εκπ}(\lambda a_1, \ldots, \lambda a_n) \mid |\lambda|\, m$. Επιπροσθέτως,

$$\lambda a_j \mid \text{εκπ}(\lambda a_1, \ldots, \lambda a_n) \Longrightarrow a_j \mid \tfrac{\text{εκπ}(\lambda a_1, \ldots, \lambda a_n)}{|\lambda|},\ \forall j \in \{1, \ldots, n\},$$

οπότε $m \mid \frac{\text{εκπ}(\lambda a_1, \ldots, \lambda a_n)}{|\lambda|} \Longrightarrow |\lambda|\, m \mid \text{εκπ}(\lambda a_1, \ldots, \lambda a_n)$. Επομένως,

$$\left.\begin{array}{r} |\lambda|\, m \mid \text{εκπ}(\lambda a_1, \ldots, \lambda a_n) \\ \text{εκπ}(\lambda a_1, \ldots, \lambda a_n) \mid |\lambda|\, m \end{array}\right\} \Longrightarrow \text{εκπ}(\lambda a_1, \ldots, \lambda a_n) = |\lambda|\, m.$$

(ii) Επειδή για κάθε $j \in \{1, \ldots, n\}$ έχουμε $\text{μκδ}(\frac{m}{a_1}, \ldots, \frac{m}{a_n}) \mid \frac{m}{a_j}$,

$$\exists c_j \in \mathbb{Z} : m = \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}) a_j c_j \Rightarrow \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}) a_j \mid m,$$

οπότε (βάσει τής προτάσεως 2.2.21)

$$\text{εκπ}\left(\text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}) a_1, \ldots, \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}) a_n\right) \mid m,$$

που σημαίνει, λόγω τού (i), ότι

$$\text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}) m \mid m \Longrightarrow \text{μκδ}(\tfrac{m}{a_1}, \ldots, \tfrac{m}{a_n}) m \leq m.$$

Κατά συνέπειαν, $\text{μκδ}(\frac{m}{a_1}, \ldots, \frac{m}{a_n}) = 1$. □

2.2.23 Πρόταση. *Εάν* $n \in \mathbb{N},\ n \geq 3$, *και εάν οι* $a_1, \ldots, a_n$ *είναι μη μηδενικοί ακέραιοι,τότε για κάθε* $k \in \mathbb{Z}$, $1 \leq k \leq n-2$, *ισχύει η ισότητα* :

$$\boxed{\text{εκπ}(a_1, \ldots, a_n) = \text{εκπ}(a_1, \ldots, a_k, \text{εκπ}(a_{k+1}, \ldots, a_n)).} \tag{2.10}$$

ΑΠΟΔΕΙΞΗ. Επειδή $a_j \mid \text{εκπ}(a_1, \ldots, a_n)$ για κάθε $j \in \{k+1, \ldots, n\}$ έχουμε

$$\text{εκπ}(a_{k+1}, \ldots, a_n) \mid \text{εκπ}(a_1, \ldots, a_n).$$

Επομένως, $a_j \mid \text{εκπ}(a_1, \ldots, a_n)$ για οιονδήποτε δείκτη $j \in \{1, \ldots, n\}$ και

$$\text{εκπ}(a_{k+1}, \ldots, a_n) \mid \text{εκπ}(a_1, \ldots, a_n),$$

απ' όπου συνάγουμε ότι

$$\text{εκπ}(a_1, \ldots, a_k, \text{εκπ}(a_{k+1}, \ldots, a_n)) \mid \text{εκπ}(a_1, \ldots, a_n). \tag{2.11}$$

Και αντιστρόφως· $\text{μκδ}(a_1, \ldots, a_k, \text{μκδ}(a_{k+1}, \ldots, a_n)) \mid a_j$ για κάθε $j \in \{1, \ldots, k\}$ και

$$\text{εκπ}(a_{k+1}, \ldots, a_n) \mid \text{εκπ}(a_1, \ldots, a_k, \text{εκπ}(a_{k+1}, \ldots, a_n)),$$

οπότε $a_j \mid \text{εκπ}(a_1, \ldots, a_k, \text{εκπ}(a_{k+1}, \ldots, a_n))$ για κάθε $j \in \{1, \ldots, n\}$, που σημαίνει ότι

$$\text{εκπ}(a_1, \ldots, a_n) \mid \text{εκπ}(a_1, \ldots, a_k, \text{εκπ}(a_{k+1}, \ldots, a_n)). \tag{2.12}$$

Επειδή τα προκείμενα ελάχιστα κοινά πολλαπλάσια είναι θετικοί ακέραιοι, από τις (2.11), (2.12) και το (iii) τής προτάσεως 2.1.5 συμπεραίνουμε την ισχύ τής ισότητας (2.10). □

2.2.24 Παρατήρηση. Θέτοντας $k = 1$ και εφαρμόζοντας τον τύπο (2.10) $n-1$ φορές είναι δυνατή η αναγωγή τής ευρέσεως τού ελαχίστου κοινού πολλαπλασίου $n \geq 3$ μη μηδενικών ακεραίων αριθμών $a_1, \ldots, a_n$ στην εύρεση τού ελαχίστου κοινού πολλαπλασίου $n-1$ *ζευγών* μη μηδενικών ακεραίων. Επιπροσθέτως, ο υπολογισμός τού ελαχίστου κοινού πολλαπλασίου *δύο* μη μηδενικών ακεραίων μπορεί να αναχθεί απευθείας στον υπολογισμό τού μεγίστου κοινού διαιρέτη τους, εάν ληφθεί υπ' όψιν ο τύπος (2.13), τον οποίο αποδεικνύουμε στην επόμενη πρόταση.

2.2.25 Πρόταση. *Για οιουσδήποτε μη μηδενικούς ακεραίους αριθμούς* a, b *έχουμε*

$$\boxed{\text{μκδ}(a,b)\ \text{εκπ}(a,b) = |ab|\,.} \tag{2.13}$$

ΑΠΟΔΕΙΞΗ. Επειδή μκδ$(a,b) \mid a$ και μκδ$(a,b) \mid b$, έχουμε μκδ$(a,b) \mid |ab|$. Αρκεί λοιπόν να αποδείξουμε ότι ο ακέραιος μη μηδενικός αριθμός $\frac{|ab|}{\text{μκδ}(a,b)}$ ισούται με το εκπ(a,b). Προς τούτο θα χρησιμοποιήσουμε την πρόταση 2.2.21. Κατ' αρχάς, $a \mid \frac{|ab|}{\text{μκδ}(a,b)}$ και $b \mid \frac{|ab|}{\text{μκδ}(a,b)}$. Ας υποθέσουμε ότι ο μ είναι ενας θετικός ακέραιος, για τον οποίο ισχύει $a \mid \mu$ και $b \mid \mu$. Κατά το θεώρημα 2.2.5, υπάρχουν ακέραιοι αριθμοί s, t, τέτοιοι ώστε να ισχύει η ισότητα: μκδ$(a,b) = sa + tb$. Συνεπώς,

$$\frac{\mu}{\frac{|ab|}{\text{μκδ}(a,b)}} = \frac{\text{μκδ}(a,b)\mu}{|ab|} = \frac{(sa+tb)\,\mu}{|ab|} = \left(\text{sign}\,(a)\,\frac{\mu}{b}\right) s + \left(\text{sign}\,(b)\,\frac{\mu}{a}\right) t \in \mathbb{Z},$$

πράγμα που σημαίνει ότι $\frac{|ab|}{\text{μκδ}(a,b)} \mid \mu$, οπότε κατ' ανάγκην $\frac{|ab|}{\text{μκδ}(a,b)} = \text{εκπ}(a,b)$. □

2.3 ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

2.3.1 Ορισμός. Ένας θετικός ακέραιος αριθμός $p > 1$ καλείται **πρώτος** όταν οι μόνοι διαιρέτες του είναι οι ± 1 και $\pm p$. Ένας πρώτος αριθμός που είναι διαιρέτης ενός ακεραίου m καλείται **πρώτος διαιρέτης** ή **πρώτος παράγοντας** τού m. Ένας φυσικός αριθμός $n \geq 2$, ο οποίος δεν είναι πρώτος, καλείται **σύνθετος αριθμός**. Εάν ο n είναι σύνθετος, τότε υπάρχουν φυσικοί αριθμοί n_1, n_2, τέτοιοι ώστε να ισχύει $1 < n_1 \leq n_2 < n$ και $n = n_1 n_2$.

2.3.2 Πρόταση. *Κάθε φυσικός αριθμός $n \geq 2$ διαθέτει τουλάχιστον έναν πρώτο διαιρέτη.*

ΑΠΟΔΕΙΞΗ. Έστω $k := \min\{\, m \in \mathbb{N} \mid m \geq 2 \text{ και } m \mid n\}$. Εάν ο k ήταν σύνθετος αριθμός, τότε θα υπήρχαν $k_1, k_2 \in \mathbb{N}$, τέτοιοι ώστε να ισχύει $2 \leq k_1 \leq k_2 < k$ και $k = k_1 k_2$, πράγμα άτοπο (αφού $k_1 \mid k$ και $k_2 \mid k$), διότι ο k είναι εξ υποθέσεως ο *ελάχιστος* φυσικός ≥ 2 με αυτήν την ιδιότητα. Άρα ο k οφείλει να είναι πρώτος αριθμός. □

2.3.3 Θεώρημα. *Το σύνολο των πρώτων αριθμών είναι ένα απειροσύνολο*[5].

ΑΠΟΔΕΙΞΗ[6]. Ας υποθέσουμε ότι το σύνολο των πρώτων αριθμών είναι πεπερασμένο, ας πούμε το $\{p_1, p_2, \ldots, p_k\}$, κι ας θεωρήσουμε τον φυσικό αριθμό

$$m := p_1 p_2 \cdots p_k + 1.$$

Τότε $p_1 \nmid m,\ p_2 \nmid m, \ldots,\ p_k \nmid m$ (διότι εάν υπήρχε κάποιος $j \in \{1, ..., k\}$ με $p_j \mid m$, θα είχαμε $p_j \mid p_1 p_2 \cdots p_k$, οπότε $p_j \mid m - p_1 p_2 \cdots p_k$, ήτοι $p_j \mid 1$, κάτι που θα

[5] Το σύνολο των πρώτων αριθμών, όντας υποσύνολο τού $\mathbb{N}$, είναι προφανώς *αριθμήσιμο*.

[6] Βλ. Ευκλείδου «Στοιχεία», βιβλίο IX, εδ. 20: «Οι πρώτοι αριθμοί πλείους εισί παντός τού προτεθέντος πλήθους πρώτων». (Πρβλ. Μετάφραση-σχόλια-επεξηγήσεις Ε. Σταμάτη, ΟΕΔΒ, Αθήνα, 1953, σελ. 250-253 και 358-359.)

αντέφασκε προς την ανισότητα $p_j \geq 2$). Τούτο όμως είναι άτοπο επί τη βάσει τής προτάσεως 2.3.2. □

2.3.4 Θεώρημα. *Κάθε φυσικός αριθμός $n \geq 2$ γράφεται ως γινόμενο πρώτων αριθμών.*

ΑΠΟΔΕΙΞΗ[7]. Θα γίνει χρήση τής δεύτερης μορφής τής μαθηματικής επαγωγής (βλ. 1.6.38). Για $n = 2$ το θεώρημα είναι αληθές. Υποθέτουμε ότι αυτό συμβαίνει και για τους ακεραίους $2, 3, \ldots, n-1$ και θεωρούμε τον ακέραιο n. Εάν ο n είναι πρώτος, τότε το θεώρημα είναι προφανώς αληθές. Εάν ο n είναι σύνθετος, τότε υπάρχουν φυσικοί αριθμοί n_1, n_2, τέτοιοι ώστε να ισχύει $1 < n_1 \leq n_2 < n$ και $n = n_1 n_2$. Λογω τής επαγωγικής υποθέσεώς μας αμφότεροι οι n_1, n_2 παριστώνται ως γινόμενα πρώτων αριθμών. Κατά συνέπειαν, και σε αυτήν την περίπτωση, ο n γράφεται ως γινόμενο πρώτων αριθμών. □

Στην επόμενη ενότητα (και συγκεκριμένα, στο θεώρημα 2.4.40) θα δοθεί μια ικανή και αναγκαία συνθήκη, ούτως ώστε ένας ακέραιος > 1 να είναι *πρώτος*.

2.3.5 Λήμμα. *Εάν οι m, n είναι ακέραιοι $\neq 0, 1$ και ο p πρώτος με $p \mid mn$, τότε είτε $p \mid m$ είτε $p \mid n$.*

ΑΠΟΔΕΙΞΗ. Εάν υποθέσουμε, χωρίς βλάβη τής γενικότητας, ότι $p \nmid m$, τότε μκδ$(p, m) = 1$, οπότε κατ' ανάγκην $p \mid n$ βάσει τού πορίσματος 2.2.10. □

2.3.6 Λήμμα. *Εάν $k \in \mathbb{N}$ και οι $p, p_1, \ldots, p_k$ είναι πρώτοι αριθμοί, τέτοιοι ώστε $p \mid p_1 \cdots p_k$, τότε υπάρχει κάποιος δείκτης $j \in \{1, ..., k\}$, με $p = p_j$.*

ΑΠΟΔΕΙΞΗ. Επειδή $p \mid p_1 \cdots p_k$, είτε $p \mid p_1$ είτε $p \mid p_2 p_3 \cdots p_k$ (βλ. 2.3.5). Εάν $p \nmid p_1$, τότε $p \mid p_2 p_3 \cdots p_k$, οπότε και πάλι είτε $p \mid p_2$ είτε $p \mid p_3 \cdots p_k$. Κατ' αναλογίαν, εάν $p \nmid p_2$, τότε $p \mid p_3 \cdots p_k$, οπότε ύστερα από την επανάληψη τού ιδίου συλλογισμού (το πολύ $k-1$ φορές) συμπεραίνουμε ότι $p \mid p_j$ για κάποιον δείκτη $j \in \{1, ..., k\}$. Επειδή οι p, p_j είναι πρώτοι, συνάγουμε ότι $p = p_j$. □

2.3.7 Θεώρημα. (Θεμελιώδες Θεώρημα τής Αριθμητικής) *Κάθε φυσικός αριθμός $n \geq 2$ γράφεται* μονοσημάντως *ως γινόμενο πρώτων αριθμών (μη λαμβανομένης υπ' όψιν τής διατάξεως των εμφανιζομένων παραγόντων εντός αυτού).*

ΑΠΟΔΕΙΞΗ. Κάτα το θεώρημα 2.3.4 κάθε φυσικός αριθμός $n \geq 2$ μπορεί να παρασταθεί ως γινόμενο πρώτων αριθμών. Αρκεί λοιπόν να αποδειχθεί το *μονοσήμαντο*

[7] Βλ. Ευκλείδου «Στοιχεία», βιβλίο VII, εδ. 31: «Άπας σύνθετος αριθμός υπό πρώτου τινός αριθμού μετρείται». (Πρβλ. Μετάφραση-σχόλια-επεξηγήσεις Ε. Σταμάτη, ΟΕΔΒ, Αθήνα, 1953, σελ. 168-171 και 322.)

τής παραστάσεως (μη λαμβανομένης υπ' όψιν τής διατάξεως των εμφανιζομένων παραγόντων εντός αυτής). Προς τούτο υποθέτουμε ότι

$$n = p_1 \cdots p_k = q_1 \cdots q_l, \tag{2.14}$$

όπου $k, l \in \mathbb{N}$ και $p_1, \ldots, p_k, q_1, \ldots, q_l$ πρώτοι αριθμοί. Επιπροσθέτως, χωρίς βλάβη τής γενικότητας, υποθέτουμε ότι

$$p_1 \leq \cdots \leq p_k \text{ και } q_1 \leq \cdots \leq q_l.$$

Χρησιμοποιώντας τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς τον n (βλ. 1.6.38) θα δείξουμε ότι

$$k = l \text{ και } p_j = q_j,\ \forall j \in \{1, \ldots, k\}.$$

Για $n = 2$ το θεώρημα είναι αληθές. Υποθέτουμε ότι αυτό είναι αληθές και για κάθε φυσικό t, με $2 \leq t < n$, όπου n οιοσδήποτε παγιωμένος φυσικός ≥ 3. Εάν ο n είναι πρώτος, τότε ο ισχυρισμός είναι αληθής. Εάν ο n είναι σύνθετος, τότε στην (2.14) έχουμε $k \geq 2$ και $l \geq 2$. Επειδή

$$p_1 \mid q_1 \cdots q_l \text{ και } q_1 \mid p_1 \cdots p_k,$$

υπάρχουν κάποιοι δείκτες $j \in \{1, ..., k\}$, $\varrho \in \{1, ..., l\}$ με $q_1 = p_j$ και $p_1 = q_\varrho$ (κατά το λήμμα 2.3.6). Εξ αυτού έπεται ότι

$$\left.\begin{array}{l} p_1 \leq p_j = q_1 \\ q_1 \leq q_\varrho = p_1 \end{array}\right\} \Longrightarrow p_1 = q_1,$$

οπότε $1 < \frac{n}{p_1} < n$ και

$$\frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_l.$$

Λόγω τής επαγωγικής υποθέσεώς μας $k - 1 = l - 1$ και $p_j = q_j, \forall j \in \{2, \ldots, k\}$. Ως εκ τούτου, $k = l$ και $p_j = q_j, \forall j \in \{1, \ldots, k\}$. □

2.3.8 Ορισμός. Από το θεώρημα 2.3.7 έπεται ότι κάθε φυσικός αριθμός $n \geq 2$ μπορεί να γραφεί *μονοσημάντως* ως

$$\boxed{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},} \tag{2.15}$$

όπου $k \in \mathbb{N}$, οι $p_1, p_2, \ldots, p_k$ πρώτοι αριθμοί με $p_1 < p_2 < \cdots < p_k$ και οι $\alpha_1, \alpha_2, \ldots, \alpha_k$ φυσικοί αριθμοί. Η έκφραση (2.15) καλείται **παράσταση τού** n **ως γινομένου πρώτων αριθμών** ή **αποσύνθεση τού** n **σε γινόμενο πρώτων αριθμών** (ή **πρώτων παραγόντων**).

2.3.9 Παρατήρηση. Προφανώς κάθε *ακέραιος* $n \in \mathbb{Z}\setminus\{0, \pm 1\}$ μπορεί να γραφεί *μονοσημάντως* ως

$$n = \text{sign}\,(n)\ p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{2.16}$$

όπου $k \in \mathbb{N}$, οι $p_1, p_2, \ldots, p_k$ πρώτοι αριθμοί με $p_1 < \cdots < p_k$ και οι $\alpha_1, \ldots, \alpha_k$ φυσικοί αριθμοί. Αλλά ακόμη και κάθε *ρητός* αριθμός $n \in \mathbb{Q}\setminus\{0, \pm 1\}$ μπορεί να παρασταθεί *μονοσημάντως* υπό τη μορφή (2.16), όπου -εν προκειμένω- οι $\alpha_1, \alpha_2, \ldots, \alpha_k$ συμβολίζουν μη μηδενικούς *ακεραίους* αριθμούς.

2.3.10 Λήμμα. *Έστω a ένας φυσικός αριθμός γραφόμενος υπό τη μορφή*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

όπου $k \in \mathbb{N}$, οι $p_1, p_2, \ldots, p_k$ διακεκριμένοι πρώτοι αριθμοί και οι $\alpha_1, \alpha_2, \ldots, \alpha_k$ μη αρνητικοί ακέραιοι αριθμοί. Τότε ένας φυσικός αριθμός b διαιρεί τον a εάν και μόνον εάν

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

όπου οι $\beta_1, \beta_2, \ldots, \beta_k$ είναι μη αρνητικοί ακέραιοι αριθμοί με $0 \le \beta_j \le \alpha_j$, για κάθε $j \in \{1, ..., k\}$.

ΑΠΟΔΕΙΞΗ. Επειδή για $a = 1$ ο ισχυρισμός είναι προφανής, μπορούμε, δίχως βλάβη τής γενικότητας, να υποθέσουμε ότι $a \ge 2$ και ότι η ανωτέρω έκραση είναι η αποσύνθεση τού a σε γινόμενο πρώτων αριθμών. Εάν $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ με $0 \le \beta_j \le \alpha_j$ για κάθε $j \in \{1, ..., k\}$, τότε

$$a = b\left(p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \cdots p_k^{\alpha_k-\beta_k}\right) \Longrightarrow b \mid a.$$

Και αντιστρόφως· εάν ο b είναι ένας φυσικός αριθμός ≥ 2, ο οποίος διαιρεί τον a και έχει ως αποσύνθεσή του σε γινόμενο πρώτων την

$$b = q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_l^{\gamma_l},$$

τότε υπάρχει φυσικός αριθμός c, τέτοιος ώστε να ισχύει η ισότητα

$$a = bc \Longrightarrow a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \left(q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_l^{\gamma_l}\right) c.$$

Από τη μοναδικότητα τής παραστάσεως τού a ως γινομένου πρώτων παραγόντων λαμβάνουμε $l \le k$ και

$$q_\varrho = p_{j_\varrho},\ 0 < \gamma_\varrho \le \alpha_{j_\varrho},\ \ \forall \varrho \in \{1, ..., l\},$$

για κάποιο υποσύνολο δεικτών $\{j_1, \ldots, j_\varrho\} \subseteq \{1, ..., k\}$. Ως εκ τούτου, οιοσδήποτε φυσικός αριθμός $b \ge 1$ διαιρεί τον a θα γράφεται υπό την επιθυμητή μορφή. □

2.3.11 Ορισμός. Ένας $a \in \mathbb{Z}\setminus\{0\}$ καλείται **τέλειο τετράγωνο** όταν $\exists c \in \mathbb{Z}\setminus\{0\}$: $c^2 = a$.

2.3.12 Πρόταση. *Εάν ένας $n \in \mathbb{N}$ δεν είναι τέλειο τετράγωνο, τότε η τετραγωνική του ρίζα $\sqrt{n}$ είναι ένας άρρητος αριθμός.*

ΑΠΟΔΕΙΞΗ. Εργαζόμαστε με «εις άτοπον απαγωγή». Υποθέτουμε ότι ο $n \in \mathbb{N}$ δεν είναι τέλειο τετράγωνο και ότι υπάρχουν $a, b \in \mathbb{Z}\setminus\{0\}$, τέτοιοι ώστε να ισχύει η ισότητα $\sqrt{n} = \frac{a}{b}$. Προφανώς, $n \geq 2$ και $n = \frac{a^2}{b^2}$. Θεωρούμε τη μοναδική παράσταση των a, b υπό τη μορφή γινομένων

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \;\; b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

όπου $k \in \mathbb{N}$, $p_1, \ldots, p_k$ διακεκριμένοι πρώτοι και $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k$ μη αρνητικοί ακέραιοι αριθμοί. Τότε

$$a^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_k^{2\alpha_k}, \;\; b^2 = p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_k^{2\beta_k}.$$

Εξ υποθέσεως, $b^2 \mid a^2$. Κατά το λήμμα 2.3.10, $0 \leq 2\beta_j \leq 2\alpha_j, \forall j \in \{1, ..., k\}$. Επομένως,

$$n = p_1^{2\alpha_1 - 2\beta_1} p_2^{2\alpha_2 - 2\beta_2} \cdots p_k^{2\alpha_k - 2\beta_k} = \left(p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \cdots p_k^{\alpha_k - \beta_k}\right)^2,$$

κάτι που καταφανώς αντιφάσκει προς την υπόθεσή μας (ήτοι προς το ότι ο n δεν είναι τέλειο τετράγωνο). □

2.3.13 Πρόταση. *Εάν $n \in \mathbb{N},\ n \geq 2$, και οι $a_1, \ldots, a_n$ είναι μη μηδενικοί ακέραιοι με*

$$|a_1| = p_1^{\alpha_{1,1}} \cdots p_k^{\alpha_{1,k}}, \ldots\ldots, \; |a_n| = p_1^{\alpha_{n,1}} \cdots p_k^{\alpha_{n,k}},$$

όπου οι $p_1, \ldots, p_k$ είναι πρώτοι αριθμοί και οι $\alpha_{j,l},\ j \in \{1, ..., n\},\ l \in \{1, ..., k\}$, μη αρνητικοί ακέραιοι αριθμοί, τότε

$$\boxed{\text{μκδ}(a_1, \ldots, a_n) = \prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}}.} \tag{2.17}$$

ΑΠΟΔΕΙΞΗ. Επειδή $\text{μκδ}(a_1, \ldots, a_n) = \text{μκδ}(|a_1|, \ldots, |a_n|)$, μπορούμε -δίχως βλάβη τής γενικότητας- να υποθέσουμε ότι οι $a_1, \ldots, a_n$ είναι θετικοί. Επειδή

$$\min\{\alpha_{1,l}, ..., \alpha_{n,l}\} \leq \alpha_{j,l}, \;\; \forall j \in \{1, ..., n\} \;\text{ και }\; \forall l \in \{1, ..., k\},$$

έχουμε $\prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l},\ldots,\alpha_{n,l}\}} \mid a_j$, για κάθε $j \in \{1,...,n\}$ (βλ. 2.3.10). Επιπροσθέτως, εάν δ είναι οιοσδήποτε φυσικός αριθμός, για τον οποίο ισχύει $\delta \mid a_1, \ldots, \delta \mid a_n$, τότε, κατά το λήμμα 2.3.10, $\delta = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$, όπου

$$0 \leq \delta_l \leq \alpha_{j,l}, \quad \forall j \in \{1,...,n\} \text{ και } \forall l \in \{1,...,k\},$$

οπότε

$$\delta_l \leq \min\{\alpha_{1,l},...,\alpha_{n,l}\}, \ \ \forall l \in \{1,...,k\} \Longrightarrow \delta \mid \prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l},\ldots,\alpha_{n,l}\}}.$$

Επομένως η (2.17) είναι αληθής λόγω τού πορίσματος 2.2.6. □

2.3.14 Πόρισμα. *Εάν $n \in \mathbb{N}$, $n \geq 2$, και οι $a, b_1, \ldots, b_n$ είναι μη μηδενικοί ακέραιοι με τους $b_1, \ldots, b_n$ σχετικώς πρώτους ανά δύο, τότε*

$$\text{μκδ}(a, \prod_{j=1}^{n} b_j) = \prod_{j=1}^{n} \text{μκδ}(a, b_j). \tag{2.18}$$

ΑΠΟΔΕΙΞΗ. Αρκεί να αποδείξουμε την ισότητα (2.18) στην περίπτωση κατά την οποία οι ως άνω αριθμοί είναι φυσικοί ≥ 2. Εφαρμόζουμε την πρώτη μορφή τής μαθηματικής επαγωγής ως προς τον n (βλ. 1.6.36), θεωρώντας ως αφετηρία μας τον $n = 2$. Εάν $n = 2$ και εάν οι αποσυνθέσεις των b_1, b_2 σε γινόμενα πρώτων παραγόντων είναι οι

$$b_1 = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad b_2 = q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_l^{\gamma_l},$$

τότε οι $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ είναι διαφορετικοί ανά δύο πρώτοι αριθμοί, καθόσον μκδ$(b_1, b_2) = 1$. Γράφοντας τον a ως γινόμενο διακεκριμένων πρώτων αριθμών υπό τη μορφή

$$a = \left(p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}\right) \left(q_1^{\varepsilon_1} q_2^{\varepsilon_2} \cdots q_l^{\varepsilon_l}\right) \left(r_1^{\zeta_1} r_2^{\zeta_2} \cdots r_m^{\zeta_m}\right),$$

όπου δ_1,$\delta_2, \ldots, \delta_k, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_l \in \mathbb{N}_0$ κατάλληλοι εκθέτες των πρώτων που εμφανίζονται στις αποσυνθέσεις των b_1, b_2 και $r_1, r_2, \ldots, r_m$ οι πρώτοι που εμφανίζονται στην αποσύνθεση τού a, αλλά δεν περιέχονται στις αποσυνθέσεις των b_1, b_2, υψωμένοι σε κατάλληλες δυνάμεις $\zeta_1, \zeta_2, \ldots, \zeta_m \in \mathbb{N}$. Εφαρμόζοντας την (2.17) λαμβάνουμε

$$\text{μκδ}\,(a, b_1 b_2) = \left(\prod_{j=1}^{k} p_j^{\min\{\beta_j,\delta_j\}}\right) \left(\prod_{\varrho=1}^{l} p_\varrho^{\min\{\gamma_\varrho,\varepsilon_\varrho\}}\right) = \text{μκδ}\,(a, b_1)\ \text{μκδ}\,(a, b_2)\,.$$

Υποθέτοντας ότι η (2.18) είναι αληθής για κάποιον $n = k \geq 2$, θα την αποδείξουμε και για $n = k + 1$. Παρατηρούμε ότι μκδ$(b_1 b_2 \cdots b_k, b_{k+1}) = 1$ (Πράγματι· εάν ο p

είναι ένας πρώτος αριθμός ο οποίος διαιρεί αμφοτέρους τους $b_1 b_2 \cdots b_k$ και b_{k+1}, τότε υπάρχει κάποιος δείκτης $j \in \{1, \ldots, k\}$ με $p \mid b_j$, οπότε $p \mid \text{μκδ}(b_j, b_{k+1}) = 1$, πράγμα άτοπο.) Βάσει των όσων αποδείξαμε για δύο παράγοντες,

$$\text{μκδ}(a, \prod_{j=1}^{k+1} b_j) = \text{μκδ}(a, \prod_{j=1}^{k} b_j)\ \text{μκδ}\,(a, b_{k+1})\,.$$

Εξάλλου, από την επαγωγική μας υπόθεση,

$$\text{μκδ}(a, \prod_{j=1}^{k} b_j) = \prod_{j=1}^{k} \text{μκδ}(a, b_j),$$

οπότε η (2.18) είναι αληθής και για $n = k + 1$. □

2.3.15 Πόρισμα. *Εστω ότι $n \in \mathbb{N},\ n \geq 2$, και ότι οι $a, b_1, \ldots, b_n$ είναι μη μηδενικοί ακέραιοι με τους $b_1, \ldots, b_n$ σχετικώς πρώτους ανά δύο. Εάν $b_j \mid a$ για κάθε δείκτη $j \in \{1, ..., n\}$, τότε $\prod_{j=1}^{n} b_j \mid a$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το πόρισμα 2.3.14 έχουμε

$$\text{μκδ}(a, \prod_{j=1}^{n} b_j) = \prod_{j=1}^{n} \text{μκδ}(a, b_j) = \prod_{j=1}^{n} |b_j|\,,$$

οπότε $\prod_{j=1}^{n} b_j \mid a$. □

2.3.16 Πόρισμα. *Εάν $n \in \mathbb{N},\ n \geq 2$, και οι $a_1, \ldots, a_n$ είναι μη μηδενικοί ακέραιοι, σχετικώς πρώτοι ανά δύο, τότε* $\text{εκπ}(a_1, \ldots, a_n) = |a_1 \cdots a_n|$.

ΑΠΟΔΕΙΞΗ. Επειδή $a_j \mid |a_1 \cdots a_n|$ για κάθε $j \in \{1, \ldots, n\}$ έχουμε

$$\text{εκπ}(a_1, \ldots, a_n) \mid |a_1 \cdots a_n|$$

(βλ. 2.2.21 (ii)). Εξάλλου επειδή εξ ορισμού $a_j \mid \text{εκπ}(a_1, \ldots, a_n)$ για κάθε δείκτη $j \in \{1, \ldots, n\}$ και οι $a_1, \ldots, a_n$ είναι σχετικώς πρώτοι ανά δύο,

$$a_1 \cdots a_n \mid \text{εκπ}(a_1, \ldots, a_n) \Longrightarrow |a_1 \cdots a_n| \mid \text{εκπ}(a_1, \ldots, a_n)$$

(βλ. 2.3.15 και 2.1.5 (i)). Επειδή τόσο το $\text{εκπ}(a_1, \ldots, a_n)$ όσο και ο $|a_1 \cdots a_n|$ είναι θετικοί ακέραιοι, από το (iii) τής προτάσεως 2.1.5 συμπεραίνουμε ότι οφείλουν να είναι ίσοι. □

2.3.17 Πρόταση. *Εάν* $n \in \mathbb{N},\ n \geq 2$, *και οι* $a_1, \ldots, a_n$ *είναι μη μηδενικοί ακέραιοι με*

$$|a_1| = p_1^{\alpha_{1,1}} \cdots p_k^{\alpha_{1,k}}, \ldots\ldots,\ |a_n| = p_1^{\alpha_{n,1}} \cdots p_k^{\alpha_{n,k}},$$

όπου οι $p_1, \ldots, p_k$ *είναι πρώτοι αριθμοί και οι* $\alpha_{j,l},\ j \in \{1, ..., n\},\ l \in \{1, ..., k\}$, *μη αρνητικοί ακέραιοι αριθμοί, τότε*

$$\boxed{\text{εκπ}(a_1, \ldots, a_n) = \prod_{l=1}^{k} p_l^{\max\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}}.} \tag{2.19}$$

ΑΠΟΔΕΙΞΗ. Επειδή $\text{εκπ}(a_1, \ldots, a_n) = \text{εκπ}(|a_1|, \ldots, |a_n|)$, μπορούμε -χωρίς βλάβη τής γενικότητας- να υποθέσουμε ότι οι $a_1, \ldots, a_n$ είναι θετικοί. Επειδή

$$\alpha_{j,l} \leq \max\{\alpha_{1,l}, ..., \alpha_{n,l}\},\ \ \forall j \in \{1, ..., n\}\ \text{και}\ \forall l \in \{1, ..., k\},$$

έχουμε $a_j \mid \prod_{l=1}^{k} p_l^{\max\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}}$, για κάθε $j \in \{1, ..., n\}$ (βλ. 2.3.10). Επιπροσθέτως, εάν μ είναι οιοσδήποτε φυσικός αριθμός, για τον οποίο ισχύει $a_1 \mid \mu, \ldots, a_n \mid \mu$, τότε, κατά το λήμμα 2.3.10,

$$\mu = \left(p_1^{\mu_1} p_2^{\mu_2} \cdots p_k^{\mu_k}\right) p_{k+1}^{\mu_{k+1}} \cdots p_\nu^{\mu_\nu},$$

όπου οι $p_1, p_2, \ldots, p_k, \ldots, p_\nu$ είναι διακεκριμένοι πρώτοι αριθμοί και οι $\mu_1, \mu_2, \ldots, \mu_k, \ldots, \mu_\nu$ κατάλληλοι φυσικοί αριθμοί με

$$\alpha_{j,l} \leq \mu_l, \quad \forall j \in \{1, ..., n\}\ \text{και}\ \forall l \in \{1, ..., k\},$$

οπότε

$$\max\{\alpha_{1,l}, ..., \alpha_{n,l}\} \leq \mu_l,\ \ \forall l \in \{1, ..., k\} \Longrightarrow \prod_{l=1}^{k} p_l^{\max\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}} \mid \mu.$$

Επομένως η (2.19) είναι αληθής λόγω τής προτάσεως 2.2.21. □

2.4 ΙΣΟΤΙΜΙΕΣ

2.4.1 Ορισμός. Έστω m ένας φυσικός αριθμός. Ένας ακέραιος a ορίζεται να είναι **ισότιμος** ενός ακεραίου b **κατά μόδιο** m (ή **modulo** m), συμβολιζόμενος ως[8]

$$\boxed{a \equiv b (\mathrm{mod}\, m),}$$

[8] Ο συμβολισμός αυτός εισήχθη από τον C.-F. Gauss (1777-1855) το έτος 1801 στο έργο του «Disquisitiones Arithmeticae», στο οποίο αναπτύσσεται με σαφήνεια και αυστηρότητα ο *λογισμός των ισοτιμιών*.

όταν $m \mid a-b$. Ο m καλείται, εν προκειμένω, **το μόδιο**[9] τής ισοτιμίας. Όταν $m \nmid a-b$, τότε λέμε ότι ο a είναι **ανισότιμος** τού b κατά μόδιο m και γράφουμε $a \not\equiv b (\mathrm{mod}\, m)$.

2.4.2 Παρατήρηση. Οι κατωτέρω ιδιότητες τής διμελούς σχέσεως "$\equiv$" (επί τού $\mathbb{Z}$) απορρέουν άμεσα από τον ορισμό 2.4.1:

(i) $a \equiv 0 (\mathrm{mod}\, m) \iff m \mid a$.

(ii) Για οιουσδήποτε ακεραίους a, b έχουμε $a \equiv b (\mathrm{mod}\, 1)$.

(iii) Ο ακέραιος a είναι άρτιος $\iff a \equiv 0 (\mathrm{mod}\, 2)$.

(iv) Ο ακέραιος a είναι περιττός $\iff a \equiv 1 (\mathrm{mod}\, 2)$.

(v) Εάν $a \equiv b (\mathrm{mod}\, m)$ και $n \mid m$, για κάποιον $n \in \mathbb{N}$, τότε $a \equiv b (\mathrm{mod}\, n)$.

2.4.3 Σημείωση. Όταν $a \equiv b (\mathrm{mod}\, m)$ οι a και b ονομάζονται ενίοτε και **ισοϋπόλοιποι** κατά μόδιο m, λόγω τής επομένης προτάσεως:

2.4.4 Πρόταση. *Έχουμε $a \equiv b (\mathrm{mod}\, m)$ εάν και μόνον εάν οι a και b, διαιρούμενοι διά τού m, αφήνουν το ίδιο υπόλοιπο.*

ΑΠΟΔΕΙΞΗ. Εκτελώντας τή διαίρεση των a και b διά τού m λαμβάνουμε

$$a = \kappa m + \nu, \qquad b = \lambda m + \rho,$$

όπου $\kappa, \lambda, \nu, \rho \in \mathbb{Z}$ με $0 \leq \nu, \rho < m$. Παρατηρούμε ότι

$$a \equiv b (\mathrm{mod}\, m) \iff m \mid a-b \iff m \mid \nu - \rho.$$

Επειδή όμως $|\nu - \rho| < m$, βάσει τού (ii) τής προτάσεως 2.1.5 συμπεραίνουμε ότι $m \mid \nu - \rho \iff \nu = \rho$. □

2.4.5 Πρόταση. (Θεμελιώδεις ιδιότητες ισοτιμιών) *Έστω ότι ο m είναι ένας φυσικός αριθμός και οι a, b, c, d ακέραιοι αριθμοί. Τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $a \equiv b (\mathrm{mod}\, m)$ και $c \equiv d (\mathrm{mod}\, m)$, τότε*

$$a \pm c \equiv b \pm d (\mathrm{mod}\, m) \quad \textit{και} \quad ac \equiv bd (\mathrm{mod}\, m).$$

(ii) *Εάν $a \equiv b (\mathrm{mod}\, m)$, τότε*

$$a \pm c \equiv b \pm c (\mathrm{mod}\, m) \quad \textit{και} \quad ac \equiv bc (\mathrm{mod}\, m).$$

[9] Άλλοι συγγραφείς προτιμούν να καλούν το μόδιο **μέτρο** τής (εκάστοτε θεωρούμενης) ισοτιμίας. Προσοχή! Μη συγχέετε το (ουδέτερο) ουσιαστικό: **το μόδιο** (γερμ. **das** Modul) με το (αρσενικό) ουσιαστικό: **ο μόδιος** (γερμ. **der** Modul) που είναι όρος χρησιμοποιούμενος για να εκφράζει έναν *γενικευμένο* διανυσματικό χώρο (με τα βαθμωτά του μεγέθη ανήκοντα σε έναν δακτύλιο που δεν είναι κατ' ανάγκην σώμα.)

(iii) *Εάν* $a \equiv b(\mathrm{mod}\, m)$, *τότε*

$$a^k \equiv b^k(\mathrm{mod}\, m), \ \ \forall k \in \mathbb{N}.$$

(iv) *Εάν* $c \neq 0$, *τότε* $a \equiv b(\mathrm{mod}\, m) \Longleftrightarrow ac \equiv bc(\mathrm{mod}\, mc)$.

(v) *Εάν* $c \neq 0$, *τότε* $ac \equiv bc(\mathrm{mod}\, m) \Longleftrightarrow a \equiv b(\mathrm{mod}\, \frac{m}{\mu\kappa\delta(m,c)})$.

ΑΠΟΔΕΙΞΗ. (i) Εάν $a \equiv b(\mathrm{mod}\, m)$ και $c \equiv d(\mathrm{mod}\, m)$, τότε υπάρχουν $k_1, k_2 \in \mathbb{Z}$, τέτοιοι ώστε

$$\left.\begin{array}{l} a-b=k_1 m \\ c-d=k_2 m \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} (a \pm c)-(b \pm d)=(a-b) \pm (c-d)=(k_1 \pm k_2)m, \\ ac-bd=(bk_2+dk_1+k_1k_2m)m, \end{array}\right.$$

οπότε $a \pm c \equiv b \pm d(\mathrm{mod}\, m)$ και $ac \equiv bd(\mathrm{mod}\, m)$.

(ii) Επειδή $c \equiv c(\mathrm{mod}\, m)$, οι ισοτιμίες αυτές έπονται από το (i).

(iii) Τούτο αποδεικνύεται κάνοντας χρήση μαθηματικής επαγωγής. Για $k = 1$, ο ισχυρισμός είναι προφανής. Υποθέτοντας ότι αυτός είναι αληθής για κάποιον ακέραιο $k > 1$, έχουμε

$$\underbrace{\begin{array}{ll} a \equiv b(\mathrm{mod}\, m) & (\text{εξ υποθέσεως}) \text{ και} \\ a^k \equiv b^k(\mathrm{mod}\, m) & (\text{από την επαγωγική μας υπόθεση}) \end{array}}$$
$$\Downarrow \text{(i)}$$
$$a^{k+1} \equiv b^{k+1}(\mathrm{mod}\, m).$$

(iv) Αρκεί να παρατηρήσουμε ότι

$$m \mid a-b \Longleftrightarrow mc \mid (a-b)\, c.$$

(v) Εάν $ac \equiv bc(\mathrm{mod}\, m)$, τότε, εφαρμόζοντας το (ii) τής προτάσεως 2.2.11 και το πόρισμα 2.2.10, λαμβάνουμε

$$m \mid (a-b)c \Longrightarrow \left.\begin{array}{l} \frac{m}{\mu\kappa\delta(m,c)} \mid (a-b)\frac{c}{\mu\kappa\delta(m,c)} \\ \mu\kappa\delta(\frac{m}{\mu\kappa\delta(m,c)}, \frac{c}{\mu\kappa\delta(m,c)}) = 1 \end{array}\right\} \Longrightarrow \frac{m}{\mu\kappa\delta(m,c)} \mid a-b,$$

ήτοι $a \equiv b(\mathrm{mod}\, \frac{m}{\mu\kappa\delta(m,c)})$. Και αντιστρόφως· υποθέτοντας ότι $a \equiv b(\mathrm{mod}\, \frac{m}{\mu\kappa\delta(m,c)})$, τότε -σύμφωνα με το (iv)- $\mu\kappa\delta(m,c)\, a \equiv \mu\kappa\delta(m,c)\, b(\mathrm{mod}\, m)$. Επιπροσθέτως,

$$\mu\kappa\delta(m,c) \mid c \Longrightarrow (\exists c' \in \mathbb{Z} : c = \mu\kappa\delta(m,c)c').$$

Εάν λοιπόν εφαρμόσουμε το (ii), λαμβάνουμε

$$\mu\kappa\delta(m,c)\, c'\, a \equiv \mu\kappa\delta(m,c)\, c'\, b(\mathrm{mod}\, m),$$

ήτοι $ac \equiv bc(\mathrm{mod}\, m)$. □

2.4.6 Πόρισμα. *Έστω ότι ο m είναι ένας φυσικός αριθμός και οι a, b, c ακέραιοι αριθμοί. Εάν $c \neq 0$, $ac \equiv bc (\mathrm{mod}\, m)$ και $\mu\kappa\delta(m, c) = 1$, τότε έχουμε $a \equiv b (\mathrm{mod}\, m)$.*

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμόσουμε το (v) τής προτάσεως 2.4.5. □

2.4.7 Πόρισμα. *Έστω ότι ο p είναι ένας πρώτος αριθμός και οι a, b, c ακέραιοι αριθμοί. Εάν $c \neq 0$, $ac \equiv bc (\mathrm{mod}\, p)$ και $p \nmid c$, τότε $a \equiv b (\mathrm{mod}\, p)$.*

ΑΠΟΔΕΙΞΗ. Επειδή $p \nmid c$ και ο p είναι πρώτος, έχουμε $\mu\kappa\delta(p, c) = 1$. Κατά συνέπειαν, $a \equiv b (\mathrm{mod}\, p)$ βάσει τού πορίσματος 2.4.6. □

2.4.8 Πρόταση. *Έστω ότι οι m_1, m_2 είναι δυο φυσικοί αριθμοί και ότι οι a, b, c είναι τρεις ακέραιοι αριθμοί, για τους οποίους ισχύουν οι ισοτιμίες*

$$a \equiv b (\mathrm{mod}\, m_1), \qquad a \equiv c (\mathrm{mod}\, m_2).$$

Τότε έχουμε $b \equiv c (\mathrm{mod} \mu\kappa\delta(m_1, m_2))$.

ΑΠΟΔΕΙΞΗ. Εάν $m_1 \mid a - b$ και $m_2 \mid a - c$, τότε, θέτοντας σε εφαρμογή το (v) τής προτάσεως 2.1.5, λαμβάνουμε

$$\left.\begin{array}{r} m_1 \mid a - b \\ \mu\kappa\delta(m_1, m_2) \mid m_1 \end{array}\right\} \Longrightarrow \mu\kappa\delta(m_1, m_2) \mid a - b,$$

και

$$\left.\begin{array}{r} m_2 \mid a - c \\ \mu\kappa\delta(m_1, m_2) \mid m_2 \end{array}\right\} \Longrightarrow \mu\kappa\delta(m_1, m_2) \mid a - c.$$

Ως εκ τούτου, λόγω τής ιδιότητας (vi) τής 2.1.5, μπορούμε να συμπεράνουμε ότι

$$\mu\kappa\delta(m_1, m_2) \mid (a - b) - (a - c) \Longrightarrow \mu\kappa\delta(m_1, m_2) \mid b - c,$$

ήτοι ότι $b \equiv c (\mathrm{mod}\ \mu\kappa\delta(m_1, m_2))$. □

2.4.9 Πρόταση. *Υποθέτουμε ότι $s \in \mathbb{N},\ s \geq 2$, ότι οι $m_1, ..., m_s$ είναι φυσικοί αριθμοί και ότι οι a, b είναι δυο ακέραιοι αριθμοί. Τότε*

$$(a \equiv b (\mathrm{mod}\, m_j),\ \ \forall j \in \{1, ..., s\}) \Longleftrightarrow a \equiv b (\mathrm{mod}\ \epsilon\kappa\pi(m_1, ..., m_s))$$

ΑΠΟΔΕΙΞΗ. Εάν $a \equiv b (\mathrm{mod}\, m_j)$ για κάθε δείκτη $j \in \{1, ..., s\}$, τότε (κατά την πρόταση 2.2.21)

$$(m_j \mid a - b,\ \ \forall j \in \{1, ..., s\}) \Longrightarrow \epsilon\kappa\pi(m_1, ..., m_s) \mid a - b.$$

Και αντιστρόφως· εάν υποθέσουμε ότι εκπ$(m_1, ..., m_s) \mid a-b$ και λάβουμε υπ' όψιν ότι

$$m_j \mid \text{εκπ}(m_1, ..., m_s), \ \ \forall j \in \{1, ..., s\},$$

συμπεραίνουμε ότι $a \equiv b (\mathrm{mod}\, m_j)$ για κάθε $j \in \{1, ..., s\}$ (πρβλ. 2.1.5 (v)). □

2.4.10 Πόρισμα. *Υποθέτουμε ότι $s \in \mathbb{N},\ s \geq 2$, ότι οι $m_1, ..., m_s$ είναι φυσικοί αριθμοί, σχετικώς πρώτοι ανά δύο, και ότι οι a, b είναι δυο ακέραιοι αριθμοί. Εάν*

$$a \equiv b (\mathrm{mod}\, m_j), \ \ \forall j \in \{1, ..., s\},$$

τότε

$$a \equiv b \ (\mathrm{mod}\ (\prod_{j=1}^{s} m_j)).$$

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί η πρόταση 2.4.9 και να ληφθεί υπ' όψιν ότι εκπ$(m_1, ..., m_s) = \prod_{j=1}^{s} m_j$ (βλ. 2.3.16). □

2.4.11 Λήμμα. *Για κάθε αριθμό $n \in \mathbb{N}_0$ ας συμβολίσουμε ως $n! = 1 \cdot 2 \cdots n$ το παραγοντικό τού n, όταν $n \geq 1$, θέτοντας $0! = 1$, και ως $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ τον διωνυμικό συντελεστή τού n υπεράνω τού k, όπου $k \in \mathbb{Z}$, $0 \leq k \leq n$. Έστω p ένας πρώτος αριθμός. Τότε*

$$\binom{p}{k} \equiv 0 \ (\mathrm{mod}\, p), \quad \forall k \in \{1, ..., p-1\}. \tag{2.20}$$

ΑΠΟΔΕΙΞΗ. Επειδή για κάθε $k \in \{1, ..., p-1\}$,

$$\underbrace{\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}}_{\Downarrow}$$
$$p(p-1)\cdots(p-k+1) = 1 \cdot 2 \cdot 3 \cdots k \cdot \tbinom{p}{k},$$

έχουμε

$$\left.\begin{array}{r} p \mid 1 \cdot 2 \cdot 3 \cdots k \cdot \binom{p}{k} \\ \text{μκδ}(p, 1 \cdot 2 \cdot 3 \cdots k) = 1 \end{array}\right\} \underset{\text{(πρβλ. 2.2.10)}}{\Longrightarrow} p \mid \tbinom{p}{k},$$

το οποίο ισοδυναμεί με την ισοτιμία (2.20). □

2.4.12 Πρόταση. *Εάν οι a, b είναι δυο ακέραιοι και ο p ένας πρώτος, τότε*

$$(a+b)^p \equiv a^p + b^p (\mathrm{mod}\, p). \tag{2.21}$$

ΑΠΟΔΕΙΞΗ. Κατά τον διωνυμικό τύπο,

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

Και επειδή $\binom{p}{k} \equiv 0 (\mathrm{mod}\, p)$ για κάθε $k \in \{1, ..., p-1\}$ (βλ. λήμμα 2.4.11), η ισοτιμία (2.21) είναι αληθής. □

2.4.13 Πόρισμα. *Εάν ο p είναι ένας πρώτος αριθμός, τότε*

$$\boxed{a^p \equiv a (\mathrm{mod}\, p), \ \ \forall a \in \mathbb{Z}.} \tag{2.22}$$

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς παρατηρούμε ότι, όταν $a = 0$ ή $a = 1$, η (2.22) είναι προφανής. Εν συνεχεία αποδεικνύουμε την (2.22) για οιονδήποτε $a \geq 1$ μέσω κλασικής μαθηματικής επαγωγής. Πράγματι· υποθέτοντας ότι η (2.22) είναι αληθής για κάποιον $a \geq 1$, αυτή ισχύει και για τον $a+1$, καθότι

$$\underbrace{\begin{array}{ll} (a+1)^p \equiv a^p + 1 (\mathrm{mod}\, p) & \text{(δυνάμει τής ισοτιμίας (2.21)) και} \\ a^p \equiv a (\mathrm{mod}\, p) & \text{(από την επαγωγική μας υπόθεση)} \end{array}}$$
$$\Downarrow$$
$$(a+1)^p \equiv a + 1 (\mathrm{mod}\, p),$$

πρβλ. 2.4.5 (ii). Απομένει η απόδειξη τού πορίσματος και για οιονδήποτε ακέραιο $a < 0$. Όμως, σε αυτήν την περίπτωση, διαιρώντας τό a διά τού p, λαμβάνουμε $a \equiv r (\mathrm{mod}\, p)$ για κάποιον $r \in \mathbb{Z}$, για τον οποίο $0 \leq r \leq p-1$. Ως εκ τούτου, κάνοντας χρήση τού (iii) τής προτάσεως 2.4.5, σε συνδυασμό με ό,τι αποδείξαμε προηγουμένως, λαμβάνουμε

$$\left.\begin{array}{l} a^p \equiv r^p (\mathrm{mod}\, p) \\ r^p \equiv r (\mathrm{mod}\, p) \\ a \equiv r (\mathrm{mod}\, p) \end{array}\right\} \Longrightarrow a^p \equiv a (\mathrm{mod}\, p).$$

Συνεπώς η (2.22) είναι όντως αληθής *για κάθε* ακέραιο a. □

2.4.14 Πόρισμα. (“**Μικρό Θεώρημα**” **τού Fermat, 1640**) *Εάν ο p είναι ένας πρώτος αριθμός και ο a ένας ακέραιος, τέτοιος ώστε*[10] $p \nmid a$, *τότε*[11]

$$\boxed{a^{p-1} \equiv 1 (\mathrm{mod}\, p).} \tag{2.23}$$

[10] Εξ αυτής τής συνθήκης έπεται, ιδιαιτέρως, ότι $a \neq 0$ (βλ. 2.1.3 (i)).

[11] Ο Pierre de Fermat (1601-1665) έγραψε επ' αυτού σε ένα γράμμα του προς τον Frenicle (τον Οκτώβριο τού 1640), αλλ' ουδέποτε έδωσε μια λεπτομερή απόδειξη.

ΑΠΟΔΕΙΞΗ. Προφανής λόγω τής ισοτιμίας (2.22) και τού πορίσματος 2.4.7 (αφού μκδ$(p,a)=1$). □

2.4.15 Παράδειγμα. Δοθέντος ενός πρώτου αριθμού $p\geq 3$ υπάρχουν άπειροι φυσικοί αριθμοί n, ούτως ώστε να πληρούται η συνθήκη $p\mid n2^n+1$. Πράγματι· θέτοντας $n=(p-1)^{2k+1}$, $k=0,1,2,\ldots$ διαπιστώνουμε μέσω τής σχέσεως (2.23) για $a=2$ ότι

$$n2^n+1\equiv (p-1)^{2k+1}\left(2^{p-1}\right)^{(p-1)^{2k}}+1\equiv (-1)^{2k+1}\,1^{2k}+1\equiv 0(\mathrm{mod}\,p).$$

► **Η κατά Euler γενίκευση τού «μικρού θεωρήματος» τού Fermat**. Ο Leonhard Euler (1707-1783) παρουσίασε κατά το έτος 1760 μια γενίκευση τού θεωρήματος 2.4.14 (βλ. 2.4.21), η οποία έμελλε να παίξει καθοριστικό ρόλο για μια πληθώρα εφαρμογών, τόσον στη Θεωρία Αριθμών όσον και στην Άλγεβρα. Η απόδειξη που παρατίθεται εδώ χρησιμοποιεί μόνον στοιχειώδη τεχνικά μέσα και ορισμένα λήμματα που αφορούν στη λεγομένη *συνάρτηση φι*.

2.4.16 Ορισμός. Η απεικόνιση $\varphi:\mathbb{N}\longrightarrow\mathbb{N}$ η οριζόμενη μέσω τού τύπου

$$\boxed{\varphi(m):=\mathrm{card}\{\ell\in\mathbb{N}\mid\ \ell\leq m\ \text{και μκδ}\,(\ell,m)=1\}.}$$

καλείται **συνάρτηση φι τού Euler**. Επί παραδείγματι, $\varphi(1)=\varphi(2)=1,\ \varphi(3)=2,$ $\varphi(4)=2,\ \varphi(5)=4,\ \varphi(6)=2,\varphi(7)=6,\ \varphi(8)=4.$

2.4.17 Λήμμα. *Η συνάρτηση φι τού Euler είναι «πολλαπλασιαστική», ήτοι για $m,n\in\mathbb{N}$ ισχύει η συνεπαγωγή*

$$\text{μκδ}(m,n)=1\Longrightarrow\varphi(mn)=\varphi(m)\,\varphi(n)\,. \tag{2.24}$$

ΑΠΟΔΕΙΞΗ. Εάν $m=1$ ή $n=1$, τότε η ως άνω ισότητα είναι προφανής. Γι' αυτόν τον λόγο, υποθέτουμε από εδώ και στο εξής ότι $m\geq 2$ και $n\geq 2$. Θέτοντας

$$S:=\{1,2,...,mn\}\ \text{ και }\ S':=\{\ell\in S\mid\ \text{μκδ}\,(\ell,mn)=1\},$$

και εφαρμόζοντας το πόρισμα 2.2.9 λαμβάνουμε

$$\varphi(mn)=\mathrm{card}\,(S')=\mathrm{card}\{\ell\in S\mid\ \text{μκδ}\,(\ell,m)=1\ \text{και μκδ}\,(\ell,n)=1\}. \tag{2.25}$$

Τοποθετώντας τά στοιχεία τού S σε έναν κατάλογο m στηλών και n γραμμών ως ακολούθως:

$$\begin{array}{cccccccc}
1 & 2 & \cdots & j & \cdots & m-1 & m \\
m+1 & m+2 & \cdots & m+j & \cdots & m+(m-1) & 2m \\
2m+1 & 2m+2 & \cdots & 2m+j & \cdots & 2m+(m-1) & 3m \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
(n-1)\,m+1 & (n-1)\,m+2 & \cdots & (n-1)\,m+j & \cdots & (n-1)\,m+(m-1) & nm
\end{array}$$

διαπιστώνουμε ότι κάθε στοιχείο τού S γράφεται μονοσημάντως υπό την μορφή $mq+j$, όπου $0 \leq q \leq n-1$ και $0 \leq j \leq m-1$. Βάσει τής προτάσεως 2.2.11 (iii), $\text{μκδ}(mq+j, m) = \text{μκδ}(j, m)$, οπότε οι αριθμοί τής j-οστής στήλης τού ανωτέρω καταλόγου είναι πρώτοι προς τον m εάν και μόνον εάν ο ίδιος ο j είναι πρώτος προς τον m. Ως εκ τούτου, μόνον $\varphi(m)$ στήλες περιέχουν φυσικούς αριθμούς πρώτους προς τον m, και κάθε στοιχείο καθεμιάς εξ αυτών είναι πρώτο προς τον m. Το πρόβλημα λοιπόν είναι να αποδειχθεί ότι σε καθεμιά εξ αυτών των $\varphi(m)$ στηλών υπάρχουν ακριβώς $\varphi(n)$ αριθμοί, οι οποίοι είναι πρώτοι προς τον n (διότι τότε θα υπάρχουν εν συνόλω $\varphi(m)\,\varphi(n)$ αριθμοί από τον κατάλογό μας, οι οποίοι θα είναι πρώτοι τόσο προς τον m όσο και προς τον n, οπότε ο ισχυρισμός θα είναι αληθής).

Ας υποθέσουμε ότι οι $\varphi(m)$ στήλες, οι οποίες περιέχουν φυσικούς αριθμούς πρώτους προς τον m, είναι οι $j_1, j_2, ..., j_{\varphi(m)}$, κι ας θεωρήσουμε το σύνολο

$$S_\kappa := \{\, x_q = mq + j_\kappa \mid 0 \leq q \leq n-1 \}$$

των εν συνόλω n στοιχείων τής στήλης j_κ, για κάθε $\kappa \in \{1, 2, ..., \varphi(m)\}$. Καθένας των x_q είναι πρώτος προς τον m. Επιπροσθέτως, εάν $q, \widehat{q} \in \{0, 1, ..., n-1\}$ και $q \neq \widehat{q}$, τότε $n \nmid x_q - x_{\widehat{q}}$, διότι, υποθέτοντας ότι $n \mid x_q - x_{\widehat{q}}$ ($\iff x_q \equiv x_{\widehat{q}} (\mathrm{mod}\ n)$), θα είχαμε

$$\left.\begin{array}{r} n \mid m(q-\widehat{q}) \\ \text{μκδ}(m,n) = 1 \end{array}\right\} \underset{(\text{βλ. } 2.2.10)}{\Longrightarrow} n \mid q - \widehat{q},$$

ήτοι κάτι το άτοπο, αφού $|q - \widehat{q}| \leq n-1$ (βλ. 2.1.5 (ii)). Κατά συνέπειαν, τα x_q και $x_{\widehat{q}}$ διαιρούμενα διά τού n αφήνουν (σύμφωνα με την πρόταση 2.4.4) *διαφορετικά* υπόλοιπα, οπότε τα n στοιχεία τού S_κ μπορούν να γραφούν υπό τη μορφή

$$n\lambda_\varrho + \varrho, \quad \forall \varrho \in \mathbb{N}_0, \ \ 0 \leq \varrho \leq n-1,$$

όπου $\lambda_0, \lambda_1, ..., \lambda_{n-1}$ είναι κατάλληλοι μη αρνητικοί ακέραιοι αριθμοί. Βάσει τής προτάσεως 2.2.11 (iii), $\text{μκδ}(n\lambda_\varrho + \varrho, n) = \text{μκδ}(\varrho, n)$, οπότε

$$\text{μκδ}(n\lambda_\varrho + \varrho, n) = 1 \iff \text{μκδ}(\varrho, n) = 1.$$

Ορίζοντας ως S'_κ το σύνολο

$$S'_\kappa := \{\, \ell \in S_\kappa \mid \text{μκδ}\,(\ell, mn) = 1 \},$$

και λαμβάνοντας υπ' όψιν ότι $\text{card}(S'_\kappa) = \varphi(n)$ για κάθε $\kappa \in \{1, 2, ..., \varphi(m)\}$, καθώς και ότι

$$S_{\kappa_1} \cap S_{\kappa_2} = \varnothing \Longrightarrow S'_{\kappa_1} \cap S'_{\kappa_2} = \varnothing,$$

για οιουσδήποτε $\kappa_1, \kappa_2 \in \{1, 2, ..., \varphi(m)\}$ με $\kappa_1 \neq \kappa_2$, συμπεραίνουμε (με τη βοήθεια τού τύπου (1.72)) ότι

$$S' = \coprod_{\kappa=1}^{\varphi(m)} S'_\kappa \Longrightarrow \text{card}(S') = \sum_{\kappa=1}^{\varphi(m)} \text{card}(S'_\kappa) = \varphi(m)\,\varphi(n). \tag{2.26}$$

Η (2.26), συνδυαζόμενη με την (2.25), μας παρέχει τη ζητούμενη ισότητα (2.24). □

2.4.18 Λήμμα. *Εάν p είναι πρώτος και $k \in \mathbb{N}$, τότε*

$$\varphi\left(p^k\right) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right).$$

ΑΠΟΔΕΙΞΗ. Επειδή

$$\begin{aligned} \varphi\left(p^k\right) &= \text{card}(\{\,\ell \in \mathbb{N} \mid \ell \leq p^k \text{ και μκδ}\left(\ell, p^k\right) = 1\}) \\ &= \text{card}(\{\,\ell \in \mathbb{N} \mid \ell \leq p^k \text{ και } p \nmid \ell\}) \end{aligned}$$

και

$$\{\,\ell \in \mathbb{N} \mid \ell \leq p^k \text{ και } p \nmid \ell\} = \{1, 2, \ldots, p^k\} \setminus \{p, 2p, 3p, \ldots, \left(p^{k-1}\right)p\},$$

έχουμε $\varphi\left(p^k\right) = p^k - p^{k-1}$. □

2.4.19 Πρόταση. *Εάν $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ είναι η αποσύνθεση ενός $m \in \mathbb{N}$ σε γινόμενο πρώτων παραγόντων, τότε*

$$\boxed{\varphi(m) = \prod_{j=1}^{s}\left(p_j^{\alpha_j} - p_j^{\alpha_j - 1}\right) = m\prod_{j=1}^{s}\left(1 - \frac{1}{p_j}\right).} \tag{2.27}$$

ΑΠΟΔΕΙΞΗ. Βάσει τού λήμματος 2.4.17 έχουμε

$$\begin{aligned} \varphi(m) &= \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}) = \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2} \cdots p_s^{\alpha_s}) \\ &= \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2})\,\varphi(p_3^{\alpha_3} \cdots p_s^{\alpha_s}) \\ &= \cdots = \prod_{j=1}^{s} \varphi\left(p_j^{\alpha_j}\right). \end{aligned}$$

Ως εκ τούτου, από το λήμμα 2.4.18 συμπεραίνουμε ότι

$$\begin{aligned}\prod_{j=1}^{s}\varphi\left(p_j^{\alpha_j}\right) &= \prod_{j=1}^{s}\left(p_j^{\alpha_j}-p_j^{\alpha_j-1}\right)\\ &= \prod_{j=1}^{s}p_j^{\alpha_j}\left(1-p_j^{-1}\right)=m\prod_{j=1}^{s}\left(1-p_j^{-1}\right),\end{aligned}$$

απ' όπου έπονται οι τύποι (2.27) για τη συνάρτηση φι τού Euler. □

2.4.20 Παράδειγμα. Όταν $m=304920$, ο δεύτερος τύπος εκ των (2.27) μας παρέχει την τιμή $\varphi(m)$ ως ακολούθως:

$$\begin{aligned}\varphi(304920) &= \varphi\left(2^3\cdot 3^2\cdot 5\cdot 7\cdot 11^2\right)\\ &= 2^3\cdot 3^2\cdot 5\cdot 7\cdot 11^2\left(\tfrac{2-1}{2}\right)\left(\tfrac{3-1}{3}\right)\left(\tfrac{5-1}{5}\right)\left(\tfrac{7-1}{7}\right)\left(\tfrac{11-1}{11}\right)\\ &= 2^2\cdot 3\cdot 11\cdot 2\cdot 4\cdot 6\cdot 10=63360.\end{aligned}$$

2.4.21 Θεώρημα. (Θεώρημα τού Euler περί ισοτιμιών) *Έστω* $m\in\mathbb{N}$, $m\geq 2$, *και έστω* a *ένας ακέραιος με* μκδ$(a,m)=1$. *Τότε*

$$\boxed{a^{\varphi(m)}\equiv 1(\mathrm{mod}\, m).} \tag{2.28}$$

ΑΠΟΔΕΙΞΗ. Αρχικώς θα αποδείξουμε μέσω κλασικής μαθηματικής επαγωγής ότι

$$a^{\varphi\left(p^k\right)}\equiv 1(\mathrm{mod}\ p^k) \tag{2.29}$$

για οιονδήποτε *πρώτο* p, ο οποίος δεν διαιρεί τον a, και για οιονδήποτε φυσικό αριθμό k. Η ισοτιμία (2.29) είναι αληθής για $k=1$, καθότι εκφράζει την ισοτιμία (2.23) τού «μικρού θεωρήματος» τού Fermat. Ας προϋποθέσουμε την ισχύ τής (2.29) για κάποιον παγιωμένο $k\geq 1$, κι ας γράψουμε τον $a^{\varphi\left(p^k\right)}$ ως

$$a^{\varphi\left(p^k\right)}=1+qp^k$$

για κάποιον ακέραιο q. Επειδή $\varphi\left(p^{k+1}\right)=p^{k+1}-p^k=p(p^k-p^{k-1})$, έχουμε

$$\varphi\left(p^{k+1}\right)=p\varphi\left(p^k\right).$$

Το διωνυμικό ανάπτυγμα, σε συνδυασμό με το λήμμα 2.4.11 και το (iv) τής προτάσεως 2.4.5, μας δίδει

$$\begin{aligned}a^{\varphi\left(p^{k+1}\right)} &= a^{p\varphi\left(p^k\right)}=\left(a^{\varphi\left(p^k\right)}\right)^p=\left(1+qp^k\right)^p\\ &= 1+\tbinom{p}{1}\left(qp^k\right)+\tbinom{p}{2}\left(qp^k\right)^2+\cdots+\tbinom{p}{p-1}\left(qp^k\right)^{p-1}+\left(qp^k\right)^p\\ &\equiv 1+\tbinom{p}{1}\left(qp^k\right)(\mathrm{mod}\ p^{k+1}).\end{aligned}$$

Δεδομένου ότι

$$p \mid \binom{p}{1} \Longrightarrow p^{k+1} \mid \binom{p}{1}\left(qp^k\right),$$

η τελευταία αυτή ισοτιμία μας οδηγεί στη ζητουμένη:

$$a^{\varphi\left(p^{k+1}\right)} \equiv 1(\mathrm{mod}\ p^{k+1}).$$

Εν συνεχεία, υποθέτοντας ότι μκδ$(m,a)=1$ και ότι η

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

είναι η αποσύνθεση τού m σε γινόμενο πρώτων παραγόντων, έχουμε

$$a^{\varphi\left(p_j^{\alpha_j}\right)} \equiv 1(\mathrm{mod}\ p_j^{\alpha_j}),\ \ \forall j \in \{1,...,s\} \tag{2.30}$$

(βάσει τού ό,τι έχουμε αποδείξει προηγουμένως). Παρατηρώντας ότι το $\varphi(m)$ διαιρείται διά τού $\varphi(p_j^{\alpha_j})$ (βάσει τού λήμματος 2.4.17) έχουμε τη δυνατότητα υψώσεως αμφοτέρων των μελών τής (2.30) στη δύναμη $\frac{\varphi(m)}{\varphi(p_j^{\alpha_j})}$ (βλ. 2.4.5 (iii)), οπότε λαμβάνουμε

$$a^{\varphi(m)} \equiv 1(\mathrm{mod}\ p_j^{\alpha_j}),\ \ \forall j \in \{1,...,s\}.$$

Εάν $s=1$, τότε η (2.28) είναι αληθής. Ας υποθέσουμε λοιπόν ότι $s \geq 2$. Επειδή μκδ$(p_j^{\alpha_j}, p_\varrho^{\alpha_\varrho}) = 1$, για κάθε $j, \varrho \in \{1,...,s\}$ με $j \neq \varrho$, το πόρισμα 2.4.10 μας δίδει

$$a^{\varphi(m)} \equiv 1(\mathrm{mod}\ (\prod_{j=1}^{s} p_j^{\alpha_j})),$$

ήτοι την (2.28). □

2.4.22 Παράδειγμα. Ας υπολογίσουμε το υπόλοιπο τής διαιρέσεως τού 3^{256} διά τού 100. Επειδή μκδ$(3,100)=1$ και

$$\varphi(100) = \varphi\left(2^2 \cdot 5^2\right) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40,$$

η σχέση (2.28) μας πληροφορεί ότι $3^{40} \equiv 1(\mathrm{mod}\,100)$. Διαιρώντας τό 256 διά τού 40 λαμβάνουμε $256 = (6 \cdot 40) + 16$, οπότε

$$3^{256} \equiv \left(3^{40}\right)^6 \cdot 3^{16} \equiv 3^{16}(\mathrm{mod}\,100).$$

Ως εκ τούτου,

$$3^{16} \equiv (81)^4 \equiv (-19)^4 \equiv (361)^2 \equiv (61)^2 \equiv 21(\mathrm{mod}\,100),$$

απ' όπου έπεται ότι το 3^{256} διαιρούμενο διά τού 100 αφήνει ως υπόλοιπο το 21.

► **Το σύνολο $\mathbb{Z}_m$ και οι συνήθεις εσωτερικές πράξεις οι οριζόμενες επ' αυτού.** Το να είναι δυο ακέραιοι a, b ισοϋπόλοιποι κατά μόδιο m ($m \in \mathbb{N}$) αποτελεί μια σχέση ισοδυναμίας. Επί τού συνόλου $\mathbb{Z}_m$ των οριζομένων κλάσεων ισοδυναμίας κληρονομούνται πράξεις *προσθέσεως* και *πολλαπλασιασμού* από τις αντίστοιχες (συνήθεις) πράξεις τις θεσπισθείσες επί τού ιδίου τού $\mathbb{Z}$.

2.4.23 Πρόταση. *Η διμελής σχέση ισοτιμίας* (*κατά παγιωμένο μόδιο* $m \in \mathbb{N}$):

$$\boxed{a \sim_m b \underset{\text{ορσ}}{\Longleftrightarrow} a \equiv b (\mathrm{mod}\, m)}$$

αποτελεί μια σχέση ισοδυναμίας επί τού συνόλου $\mathbb{Z}$ των ακεραίων.

ΑΠΟΔΕΙΞΗ. Θεωρούμε τυχόντες $a, b, c \in \mathbb{Z}$. Η " $\sim_m$ " είναι ανακλαστική, διότι $a - a = 0 = 0 \cdot m$, συμμετρική, διότι

$$a - b = km \Longrightarrow b - a = (-k)\, m,$$

και μεταβατική λόγω τής συνεπαγωγής

$$\left.\begin{array}{l} a - b = k_1 m \\ b - c = k_2 m \end{array}\right\} \Longrightarrow a - c = (k_1 + k_2)\, m,$$

όπου $k, k_1, k_2 \in \mathbb{Z}$, οπότε $a \equiv a (\mathrm{mod}\, m)$, $a \equiv b (\mathrm{mod}\, m) \Longrightarrow b \equiv a (\mathrm{mod}\, m)$, και εάν $a \equiv b (\mathrm{mod}\, m)$ και $b \equiv c (\mathrm{mod}\, m)$, τότε $a \equiv c (\mathrm{mod}\, m)$. □

2.4.24 Σημείωση. (i) Όταν $a \equiv b (\mathrm{mod}\, m)$, λόγω τής συμμετρικότητας τής διμελούς σχέσεως " $\sim_m$ " μπορούμε να χαρακτηρίζουμε τους a, b ως *ισοτίμους* κατά μόδιο m, χωρίς να καταφεύγουμε σε διάκριση προτεραιότητας, ήτοι στο ποιος εξ αυτών προηγείται ή έπεται τού άλλου.

(ii) Για να δώσουμε έμφαση στην εξάρτηση από το m συμβολίζουμε ως

$$\ldots, [-2]_m, [-1]_m, [0]_m, [1]_m, [2]_m, \ldots$$

τις κλάσεις ισοδυναμίας των ακεραίων (ως προς την " $\sim_m$ ") και ως

$$\boxed{\mathbb{Z}_m := \mathbb{Z}/\sim_m}$$

το **σύνολο των κλάσεων υπολοίπων (ή κλάσεων ισοτιμίας) των ακεραίων κατά μόδιο** m (ή **modulo** m).

2.4.25 Πρόταση. *Το ανωτέρω σύνολο των κλάσεων υπολοίπων γράφεται σε «ανηγμένη» μορφή* [12] *ως ακολούθως:*

$$\boxed{\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.} \tag{2.31}$$

[12] Τούτο σημαίνει ότι τα εντός των αγκίστρων αναγραφόμενα στοιχεία είναι *σαφώς διακεκριμένα* (ήτοι ανά δύο διαφορετικά, αποκλείοντας την επανάληψη κάποιου εξ αυτών).

ΑΠΟΔΕΙΞΗ. Επειδή *κάθε* $a \in \mathbb{Z}$ μπορεί να γραφεί υπό τη μορφή $a = qm + r$, όπου τα q και r είναι κατάλληλοι ακέραιοι αριθμοί και $0 \leq r < m$ (ήτοι το r είναι το υπόλοιπο τής διαιρέσεως τού a διά τού m, βλ. (2.1)), λαμβάνουμε την ισότητα $[a]_m = [r]_m$. Εξ αυτού συνάγουμε ότι οι *σαφώς διακεκριμένες* κλάσεις ισοδυναμίας που διαθέτουμε είναι οι μόνον οι $[0]_m, [1]_m, \ldots, [m-1]_m$. □

2.4.26 Σημείωση. Χρησιμοποιώντας τήν ορολογία την εισαχθείσα στο εδάφιο 1.3 .19 διαπιστώνουμε μέσω τής προτάσεως 2.4.25 ότι το σύνολο $\{0, 1, \ldots, m-1\}$ είναι ένα *πλήρες σύστημα εκπροσώπων*[13] *τού* $\mathbb{Z}$ *ως προς την* "$\sim_m$" , οπότε

$$\mathbb{Z} = \coprod \{[j]_m \,|\, j \in \{0, 1, \ldots, m-1\}\}.$$

Προσοχή! Για κάθε $j \in \{0, 1, \ldots, m-1\}$ το $[j]_m$ είναι *ένα* στοιχείο τού $\mathbb{Z}_m$ αλλά ως υποσύνολο τού $\mathbb{Z}$ αποτελείται από *όλους τους ακεραίους που διαιρούμενοι* διά τού m *αφήνουν υπόλοιπο* j.

2.4.27 Λήμμα. *Η* "$\sim_m$" *είναι συμβατή με τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού ακεραίων αριθμών* (βλ. 1.5.19, 1.7.9).

ΑΠΟΔΕΙΞΗ. Ο ισχυρισμός είναι αληθής λόγω των ιδιοτήτων 2.4.5 (i). □

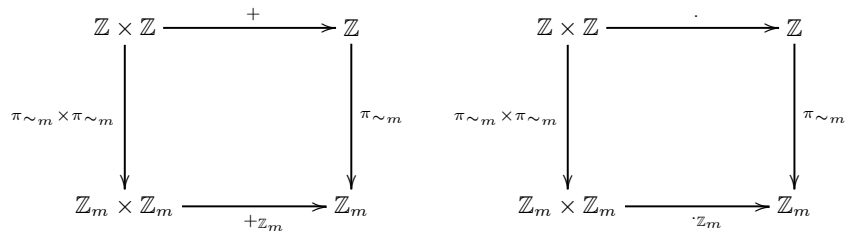
2.4.28 Θεώρημα. *Επί τού* $\mathbb{Z}_m$ *ορίζονται δύο εσωτερικές πράξεις* "$+_{\mathbb{Z}_m}$" *και* "$\cdot_{\mathbb{Z}_m}$":

$$([a]_m, [b]_m) \longmapsto [a]_m +_{\mathbb{Z}_m} [b]_m, \quad ([a]_m, [b]_m) \longmapsto [a]_m \cdot_{\mathbb{Z}_m} [b]_m$$

μέσω των τύπων

$$\boxed{\begin{array}{c} [a]_m +_{\mathbb{Z}_m} [b]_m := [a+b]_m, \\ [a]_m \cdot_{\mathbb{Z}_m} [b]_m := [ab]_m. \end{array}} \tag{2.32}$$

Αυτές είναι οι μοναδικές απεικονίσεις από το $\mathbb{Z}_m \times \mathbb{Z}_m$ *στο* $\mathbb{Z}_m$ *οι οποίες καθιστούν τα διαγράμματα*



μεταθετικά.

[13] Προφανώς, κάθε πλήρες σύστημα εκπροσώπων τού $\mathbb{Z}$ ως προς την "$\sim_m$" είναι τής μορφής $\{a_0, a_1, ..., a_{m-1}\}$, όπου $a_j \in \mathbb{Z}$ και $a_j \equiv j \pmod m$, $\forall j \in \{0, 1, \ldots, m-1\}$.

ΑΠΟΔΕΙΞΗ. Κατά το λήμμα 2.4.27 η "$\sim_m$" είναι συμβατή με τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού ακεραίων αριθμών. Ως εκ τούτου, είναι δυνατή η εφαρμογή τού θεωρήματος 1.5.20 για καθεμιά εξ αυτών και ο προσδιορισμός των μοναδικών απεικονίσεων (2.32) που καθιστούν τα ανωτέρω διαγράμματα μεταθετικά. □

2.4.29 Σημείωση. Επειδή κατά την εφαρμογή των ορισμών (2.32) οι ακέραιοι $a+b$ και ab ενδέχεται να είναι $\geq m$ (ακόμη και όταν οι a και b είναι ειλημμένοι από το σύνολο $\{0, 1, ..., m-1\}$), για να παραμείνουμε στην περιγραφή (2.31) τού $\mathbb{Z}_m$ επιλέγουμε ως εκπροσώπους των κλάσεων ισοδυναμιών τους ως προς την "$\sim_m$" τα υπόλοιπα που αφήνουν αφού διαιρεθούν διά τού m. Επί παραδείγματι, όταν $m = 6$, οι υπονοούμενοι εκπρόσωποι των *αθροισμάτων* δύο τυχόντων στοιχείων ειλημμένων από το

$$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$$

έχουν καταχωρισθεί στον ακόλουθο κατάλογο:

$+_{\mathbb{Z}_6}$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

Ο αντίστοιχος κατάλογος που περιλαμβάνει τα *γινόμενα* είναι ο εξής:

$\cdot_{\mathbb{Z}_6}$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

2.4.30 Πρόταση. (Ιδιότητες προσθέσεως) *Η πράξη "$+_{\mathbb{Z}_m}$" έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** $[a]_m +_{\mathbb{Z}_m} [b]_m = [b]_m +_{\mathbb{Z}_m} [a]_m, \forall (a, b) \in \mathbb{Z} \times \mathbb{Z}$.

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε $a, b, c \in \mathbb{Z}$ ισχύει η ισότητα*

$$([a]_m +_{\mathbb{Z}_m} [b]_m) +_{\mathbb{Z}_m} [c]_m = [a]_m +_{\mathbb{Z}_m} ([b]_m +_{\mathbb{Z}_m} [c]_m).$$

(iii) **[Νόμος τής διαγραφής]** *Για οιουσδήποτε* $a, b, c \in \mathbb{Z}$ *ισχύει η συνεπαγωγή*

$$[a]_m +_{\mathbb{Z}_m} [c]_m = [b]_m +_{\mathbb{Z}_m} [c]_m \Longrightarrow [a]_m = [b]_m.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $[0]_m$ *είναι ουδέτερο στοιχείο τού* $\mathbb{Z}_m$ *ως προς την* "$+_{\mathbb{Z}_m}$" (βλ. 1.5.6), *δηλαδή*

$$[0]_m +_{\mathbb{Z}_m} [a]_m = [a]_m = [a]_m +_{\mathbb{Z}_m} [0]_m.$$

(v) **[Ύπαρξη συμμετρικού στοιχείου]** *Κάθε* $[a]_m \in \mathbb{Z}_m$ *έχει την κλάση ισοτιμίας* $[-a]_m$ *ως συμμετρικό του στοιχείο ως προς την* "$+_{\mathbb{Z}_m}$" (βλ. 1.5.11), *δηλαδή*

$$[-a]_m +_{\mathbb{Z}_m} [a]_m = [0]_m = [a]_m +_{\mathbb{Z}_m} [-a]_m.$$

ΑΠΟΔΕΙΞΗ. Λαμβάνοντας υπ' όψιν το θεώρημα 2.4.28, τα (i), (ii), (iv) και (v) έπονται από τον συνδυασμό των (i), (ii), (iv), (v) τής προτάσεως 1.7.13 και των (b), (c), (d) και (e) τού θεωρήματος 1.5.20.

(iii) Εάν οι a, b, c είναι ακέραιοι αριθμοί, τέτοιοι ώστε να ισχύει η ισότητα

$$[a]_m +_{\mathbb{Z}_m} [c]_m = [b]_m +_{\mathbb{Z}_m} [c]_m,$$

τότε

$$[a + c]_m = [b + c]_m \Rightarrow m \mid (a + c) - (b + c) = a - b \Rightarrow [a]_m = [b]_m,$$

οπότε και ο νόμος τής διαγραφής ισχύει για το $\mathbb{Z}_m$. □

2.4.31 Πρόταση. (Ιδιότητες πολλαπλασιασμού) *Η πράξη* "$\cdot_{\mathbb{Z}_m}$" *έχει τις εξής ιδιότητες*:

(i) **[Μεταθετική ιδιότητα]** *Για οιουσδήποτε* $a, b \in \mathbb{Z}$ *ισχύει η ισότητα*

$$[a]_m \cdot_{\mathbb{Z}_m} [b]_m = [b]_m \cdot_{\mathbb{Z}_m} [a]_m.$$

(ii) **[Προσεταιριστική ιδιότητα]** *Για οιουσδήποτε* $a, b, c \in \mathbb{Z}$ *ισχύει η ισότητα*

$$([a]_m \cdot_{\mathbb{Z}_m} [b]_m) \cdot_{\mathbb{Z}_m} [c]_m = [a]_m \cdot_{\mathbb{Z}_m} ([b]_m \cdot_{\mathbb{Z}_m} [c]_m).$$

(iii) *Για οιονδήποτε* $a \in \mathbb{Z}$ *ισχύουν οι ισότητες*

$$[0]_m \cdot_{\mathbb{Z}_m} [a]_m = [0]_m = [a]_m \cdot_{\mathbb{Z}_m} [0]_m.$$

(iv) **[Ύπαρξη ουδετέρου στοιχείου]** *Το* $[1]_m$ *είναι ουδέτερο στοιχείο τού* $\mathbb{Z}_m$ *ως προς την* "$\cdot_{\mathbb{Z}_m}$" (βλ. 1.5.6), *δηλαδή*

$$[1]_m \cdot_{\mathbb{Z}_m} [a]_m = [a]_m = [a]_m \cdot_{\mathbb{Z}_m} [1]_m.$$

(v) *Για οιουσδήποτε* $a, b \in \mathbb{Z}$ *ισχύουν οι ισότητες*

$$[-a]_m \cdot_{\mathbb{Z}_m} [b]_m = [-ab]_m = [a]_m \cdot_{\mathbb{Z}_m} [-b]_m.$$

(vi) **[Επιμεριστική ιδιότητα τού πολλαπλασιασμού ως προς την πρόσθεση]** *Για οιουσδήποτε* $a, b, c \in \mathbb{Z}$ *ισχύουν οι ισότητες*

$$\begin{aligned} [a]_m \cdot_{\mathbb{Z}_m} ([b]_m +_{\mathbb{Z}_m} [c]_m) &= ([a]_m \cdot_{\mathbb{Z}_m} [b]_m) +_{\mathbb{Z}_m} ([a]_m \cdot_{\mathbb{Z}_m} [c]_m), \\ ([a]_m +_{\mathbb{Z}_m} [b]_m) \cdot_{\mathbb{Z}_m} [c]_m &= ([a]_m \cdot_{\mathbb{Z}_m} [c]_m) +_{\mathbb{Z}_m} ([b]_m \cdot_{\mathbb{Z}_m} [c]_m). \end{aligned}$$

ΑΠΟΔΕΙΞΗ. Λαμβάνοντας υπ' όψιν το θεώρημα 2.4.28, τα (i), (ii) και (iv) έπονται από τον συνδυασμό των (i), (ii), (iv) τής προτάσεως 1.7.13 και των (b), (c) και (d) τού θεωρήματος 1.5.20.

(iii) Τούτο είναι προφανές από τον ορισμό τής πράξεως "$\cdot_{\mathbb{Z}_m}$".

(v) Εφαρμόζοντας το 1.7.13 (v) λαμβάνουμε

$$\begin{aligned} [-a]_m \cdot_{\mathbb{Z}_m} [b]_m &= [(-a)\, b]_m = [-ab]_m \\ &= [a(-b)]_m = [a]_m \cdot_{\mathbb{Z}_m} [-b]_m. \end{aligned}$$

(vi) Εφαρμόζοντας το 1.7.13 (vi) λαμβάνουμε

$$\begin{aligned} [a]_m \cdot_{\mathbb{Z}_m} ([b]_m +_{\mathbb{Z}_m} [c]_m) &= [a]_m \cdot_{\mathbb{Z}_m} ([b + c]_m) \\ &= [a(b + c)]_m = [ab + ac]_m \\ &= [ab]_m +_{\mathbb{Z}_m} [ac]_m \\ &= ([a]_m \cdot_{\mathbb{Z}_m} [b]_m) +_{\mathbb{Z}_m} ([a]_m \cdot_{\mathbb{Z}_m} [c]_m). \end{aligned}$$

Η άλλη ισότητα είναι προφανής, διότι η "$\cdot_{\mathbb{Z}_m}$" (κατά το (i)) είναι μεταθετική. □

2.4.32 Πρόταση. *Ένα στοιχείο* $[a]_m$ *τού* $\mathbb{Z}_m$ *διαθέτει συμμετρικό στοιχείο*[14] *ως προς την* "$\cdot_{\mathbb{Z}_m}$" *εάν και μόνον εάν* μκδ$(a, m) = 1$.

ΑΠΟΔΕΙΞΗ. Έστω ότι το $[a]_m$ διαθέτει το $[b]_m$ ως συμμετρικό του στοιχείο ως προς την "$\cdot_{\mathbb{Z}_m}$". Τότε

$$[a]_m \cdot_{\mathbb{Z}_m} [b]_m = [ab]_m = [1]_m \Longrightarrow \exists k \in \mathbb{Z} : ab = mk + 1.$$

Τούτο, σύμφωνα με το πόρισμα 2.2.8, σημαίνει ότι μκδ$(a, m) = 1$. Και αντιστρόφως· υποθέτοντας ότι μκδ$(a, m) = 1$, θα υπάρχουν $c, d \in \mathbb{Z}$, τέτοιοι ώστε

$$\begin{aligned} &ac + md = 1 \Rightarrow [ac + md]_m = ([a]_m \cdot_{\mathbb{Z}_m} [c]_m) +_{\mathbb{Z}_m} ([m]_m \cdot_{\mathbb{Z}_m} [d]_m) = [1]_m \\ &\Longrightarrow ([a]_m \cdot_{\mathbb{Z}_m} [c]_m) = [1]_m \ \text{(λόγω τού 2.4.31 (iii) και τού ότι } [m]_m = [0]_m), \end{aligned}$$

[14] Εάν το $[a]_m$ διαθέτει συμμετρικό στοιχείο ως προς την "$\cdot_{\mathbb{Z}_m}$", τότε αυτό θα είναι μονοσημάντως ορισμένο επί τη βάσει τής προτάσεως 1.5.13. Εξάλλου, επειδή η "$\cdot_{\mathbb{Z}_m}$" είναι μεταθετική (βλ. 2.4.31 (i)), αρκεί κανείς να περιορισθεί στην εξέταση υπάρξεως εκ δεξιών συμμετρικού στοιχείου τού $[a]_m$ (βλ. 1.5.14).

απ' όπου έπεται ότι το $[a]_m$ διαθέτει το $[c]_m$ ως συμμετρικό του στοιχείο ως προς την "$\cdot_{\mathbb{Z}_m}$". □

2.4.33 Σημείωση. (Απλούστευση συμβολισμών) Υιοθετώντας, από εδώ και στο εξής, για λόγους χρηστικότητας, την «ελάφρυνση» των συμβολισμών των πράξεών μας (που έχουμε ήδη εγκαινιάσει στη σημείωση ?? για τα συνήθη αριθμητικά σύνολα), θα γράφουμε απλώς $[a]_m + [b]_m$ και $[a]_m \cdot [b]_m$ (ή $[a]_m[b]_m$) αντί των $[a]_m +_{\mathbb{Z}_m} [b]_m$ και $[a]_m \cdot_{\mathbb{Z}_m} [b]_m$, αντιστοίχως.

► **Γραμμικές ισοτιμίες**. Έστω ότι ο m είναι ένας φυσικός αριθμός και οι a, b δυο ακέραιοι αριθμοί. Κάθε ισοτιμία τής μορφής

$$\boxed{ax \equiv b(\mathrm{mod}\, m),} \tag{2.33}$$

με το x προσδιοριστέο εντός τού συνόλου των ακεραίων αριθμών, καλείται **γραμμική ισοτιμία** (με *άγνωστό της* τον x). Λέμε ότι ένας $x_0 \in \mathbb{Z}$ *πληροί* (ή *επαληθεύει*) την (2.33) όταν $ax_0 \equiv b(\mathrm{mod}\, m)$. Εν τοιαύτη περιπτώσει, *και οιοσδήποτε άλλος* εκπρόσωπος τής κλάσεως υπολοίπων $[x_0]_m$ τού x_0 επαληθεύει την (2.33). Πράγματι· εάν $y \in [x_0]_m$, τότε $[y]_m = [x_0]_m$, απ' όπου έπεται ότι $y \equiv x_0(\mathrm{mod}\, m)$, οπότε

$$ay \equiv ax_0 \equiv b(\mathrm{mod}\, m).$$

Ως εκ τούτου, όταν ομιλούμε για μια **λύση** $x_0 \in \mathbb{Z}$ **τής** (2.33) **κατά μόδιο** m, εννοούμε ολόκληρη[15] την κλάση $[x_0]_m$, όπου ο x_0 πληροί την (2.33). Επίσης, όταν εργαζόμαστε με συγκεκριμένα παραδείγματα και συναντούμε μια λύση $[x_0]_m$, για να εμπίπτουμε στην περιγραφή που δώσαμε για το σύνολο $\mathbb{Z}_m$ μέσω τής προτάσεως 2.4.25 προτιμούμε να παραθέτουμε τον *μοναδικό* εκπρόσωπο x_0' τής κλάσεως υπολοίπων $[x_0]_m$ ο οποίος ανήκει στο σύνολο $\{0, 1, \ldots, m-1\}$, ήτοι να καταφεύγουμε σε *αναγωγή* τού x_0 κατά μόδιο m κατόπιν διαιρέσεώς του διά τού m (βλ. απόδειξη τής 2.4.25).

Σημειωτέον ότι υπάρχουν γραμμικές ισοτιμίες οι οποίες δεν δέχονται καμία ακεραία λύση, όπως π.χ. η $2x \equiv 3(\mathrm{mod}\, 4)$, αφού για κάθε $k \in \mathbb{Z}$ ο ακέραιος $2k-3$ είναι περιττός και επομένως $4 \nmid 2k-3$. Η πρόταση που ακολουθεί μας γνωστοποιεί την ικανή και αναγκαία συνθήκη για την ύπαρξη ακεραίων λύσεων τής (2.33) και, επιπροσθέτως, περιγράφει τη μορφή όλων των δυνατών λύσεων.

2.4.34 Πρόταση. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, η γραμμική ισοτιμία* (2.33) *διαθέτει λύσεις $x \in \mathbb{Z}$ κατά μόδιο m εάν και μόνον εάν* μκδ$(a, m) \mid b$.

[15] Γι' αυτόν τον λόγο, δυο ακέραιες λύσεις x_1 και x_2 τής (2.33) λογίζονται ως *διαφορετικές* όταν $x_1 \not\equiv x_2(\mathrm{mod}\, m)$.

Επιπροσθέτως, όταν $\text{μκδ}\,(a,m)|\,b$, *η ισοτιμία* (2.33) *διαθέτει ακριβώς* $\text{μκδ}(a,m)$ *σαφώς διακεκριμένες λύσεις* $x\in\mathbb{Z}$ *κατά μόδιο* m, *οι οποίες είναι τής μορφής*

$$\boxed{x=x_0+k\,\frac{m}{\text{μκδ}\,(a,m)},\quad k\in\{0,1,\dots,\text{μκδ}\,(a,m)-1\},} \tag{2.34}$$

όπου x_0 *μια ειδική λύση τής* (2.33).

ΑΠΟΔΕΙΞΗ. Εάν η (2.33) δέχεται μια λύση $x\in\mathbb{Z}$ κατά μόδιο m, τότε

$$ax\equiv b(\text{mod }\,m)\Longrightarrow m\mid ax-b\Longrightarrow(\exists k\in\mathbb{Z}:b=ax-km)\,.$$

Επομένως,

$$\left.\begin{array}{c}\text{μκδ}\,(a,m)\mid a\\ \text{μκδ}\,(a,m)\mid m\end{array}\right\}\underset{(\text{βλ. 2.1.5 (vi)})}{\Longrightarrow}\text{μκδ}\,(a,m)\mid ax-km\,(=b).$$

Και αντιστρόφως· εάν $\text{μκδ}(a,m)\mid b$, τότε $b=\text{μκδ}(a,m)\,b'$ για κάποιον $b'\in\mathbb{Z}$. Επειδή, κατά το (ii) τής προτάσεως 2.2.11, ισχύει η

$$\text{μκδ}\left(\tfrac{a}{\text{μκδ}(a,m)},\tfrac{m}{\text{μκδ}(a,m)}\right)=1\underset{(\text{βλ. 2.2.8})}{\Longrightarrow}\left(\exists\kappa,\lambda\in\mathbb{Z}:\kappa\tfrac{a}{\text{μκδ}(a,m)}+\lambda\tfrac{m}{\text{μκδ}(a,m)}=1\right),$$

λαμβάνουμε

$$b=\kappa\tfrac{ab}{\text{μκδ}(a,m)}+\lambda\tfrac{mb}{\text{μκδ}(a,m)}=a\,(\kappa b')+m\,(\lambda b')\Longrightarrow a\,(\kappa b')\equiv b(\text{mod }\,m),$$

οπότε η κλάση ισοτιμίας τού $\kappa b'$ κατά μόδιο m είναι μια λύση τής (2.33).

Εν συνεχεία υποθέτουμε οτι το x_0 (ή, ακριβέστερα, η κλάση $[x_0]_m$) είναι μια παγιωμένη (ειδική) λύση τής (2.33). Προφανώς,

$$a\left(x_0+k\frac{m}{\text{μκδ}\,(a,m)}\right)=ax_0+\left(\frac{ak}{\text{μκδ}\,(a,m)}\right)m\equiv b(\text{mod }\,m),$$

οπότε οι ακέραιοι (2.34) αποτελούν πράγματι λύσεις τής (2.33). Οι ακέραιοι αυτοί είναι ανά δύο ανισότιμοι κατά μόδιο m, καθότι για οιουσδήποτε ακεραίους αριθμούς $k,k'\in\{0,1,\dots,\text{μκδ}(a,m)-1\}$ με $k\neq k'$, έχουμε

$$\left|\left(x_0+\tfrac{mk}{\text{μκδ}(a,m)}\right)-\left(x_0+\tfrac{mk'}{\text{μκδ}(a,m)}\right)\right|=|k-k'|\;\tfrac{m}{\text{μκδ}(a,m)}<m,$$

αφού $|k-k'|<\text{μκδ}(a,m)$. Συνεπώς, λόγω τού (ii) τής προτάσεως 2.1.5, έχουμε

$$\begin{array}{c}m\nmid\left(x_0+\tfrac{mk}{\text{μκδ}(a,m)}\right)-\left(x_0+\tfrac{mk'}{\text{μκδ}(a,m)}\right)\\ \Downarrow\\ \left(x_0+\tfrac{mk}{\text{μκδ}(a,m)}\right)\not\equiv\left(x_0+\tfrac{mk'}{\text{μκδ}(a,m)}\right)(\text{mod }\,m).\end{array}$$

Απομένει λοιπόν να αποδειχθεί ότι και κάθε άλλη λύση $y \in \mathbb{Z}$ τής (2.33) είναι ισότιμη με κάποια εκ των (2.34) κατά μόδιο m. Επειδή

$$\left.\begin{array}{r} ax_0 \equiv b(\mathrm{mod}\ m) \\ ay \equiv b(\mathrm{mod}\ m) \end{array}\right\} \Longrightarrow ax_0 \equiv ay(\mathrm{mod}\ m) \Longrightarrow m \mid a\,(y - x_0)\,,$$

συμπεραίνουμε ότι

$$\left.\begin{array}{c} \frac{m}{\mu\kappa\delta(a,m)} \mid \frac{a}{\mu\kappa\delta(a,m)}\,(y - x_0) \\ \mu\kappa\delta\left(\frac{a}{\mu\kappa\delta(a,m)}, \frac{m}{\mu\kappa\delta(a,m)}\right) = 1 \end{array}\right\} \Longrightarrow \begin{array}{c} \frac{m}{\mu\kappa\delta(a,m)} \mid y - x_0 \\ \Downarrow \\ \left(\exists \nu \in \mathbb{Z} : y - x_0 = \frac{m\nu}{\mu\kappa\delta(a,m)}\right). \end{array}$$

Διαιρώντας τον ν διά τού $\mu\kappa\delta(a, m)$ λαμβάνουμε ένα μονοσημάντως ορισμένο ζεύγος $(q, r) \in \mathbb{Z}^2$ με

$$\nu = \mu\kappa\delta\,(a, m)\,q + r, \quad 0 \leq r \leq \mu\kappa\delta\,(a, m) - 1.$$

Ως εκ τούτου,

$$y - x_0 = \tfrac{m(\mu\kappa\delta(a,m)q+r)}{\mu\kappa\delta(a,m)} = mq + \tfrac{rm}{\mu\kappa\delta(a,m)} \equiv \tfrac{rm}{\mu\kappa\delta(a,m)}(\mathrm{mod}\ m),$$

οπότε $y \equiv x_0 + r\frac{m}{\mu\kappa\delta(a,m)}(\mathrm{mod}\, m)$, $\forall r \in \{0, 1, \ldots, \mu\kappa\delta(a, m) - 1\}$. □

2.4.35 Πόρισμα. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, η γραμμική ισοτιμία* (2.33) *διαθέτει ακριβώς μία λύση x_0 κατά μόδιο m εάν και μόνον εάν* $\mu\kappa\delta\,(a, m) = 1$.

2.4.36 Σημείωση. Όταν $\mu\kappa\delta(a, m) = 1$, ένας τρόπος υπολογισμού τής λύσεως x_0 κατά μόδιο m διασφαλίζεται μέσω τής προσφυγής μας στον κλασικό *ευκλείδειο αλγόριθμο* (ήτοι στον προσδιορισμό ενός ζεύγους $(x_0^*, y_0^*) \in \mathbb{Z}^2$ για το οποίο ισχύει $ax_0^* - my_0^* = 1$, ορίζοντας ως x_0 το $x_0 := bx_0^*$, πρβλ. πρόταση 2.2.17). Ένας άλλος τρόπος υπολογισμού τής λύσεως x_0 είναι δυνατός κατόπιν εφαρμογής τού θεωρήματος τού Euler 2.4.21 περί ισοτιμιών. Σύμφωνα με αυτό, (λόγω τής συνθήκης $\mu\kappa\delta(a, m) = 1$) έχουμε

$$a^{\varphi(m)} \equiv 1(\mathrm{mod}\ m),$$

όπου φ η συνάρτηση φι τού Euler (βλ. 2.4.16). Ως εκ τούτου, αρκεί να θέσουμε

$$\boxed{x_0 := a^{\varphi(m)-1}b,} \tag{2.35}$$

να εφαρμόσουμε τον τύπο (2.27) για την εύρεση τού $\varphi\,(m)$ για τον δοθέντα φυσικό αριθμό m και να διενεργήσουμε αναγωγή κατά μόδιο m.

2.4.37 Παράδειγμα. Επειδή μκδ$(5, 24) = 1$, η γραμμική ισοτιμία $5x \equiv 3 (\mathrm{mod}\ 24)$ διαθέτει ακριβώς μία λύση x_0 κατά μόδιο m. Γράφοντας $24 = 2^3 \cdot 3$, ο τύπος (2.27) μας δίδει την τιμή $\varphi(24) = (2^3 - 2^2)(3 - 1) = 8$. Κατά τον (2.35), μπορούμε να θέσουμε ως $x_0 := 5^7 \cdot 3 = 234\,375$. Επειδή $234\,375 = 9765 \cdot 24 + 15$, έχουμε $[x_0]_{24} = [15]_{24}$, οπότε $5 \cdot 15 \equiv 3 (\mathrm{mod}\ 24)$.

Η εύρεση των λύσεων τής γενικής γραμμικής ισοτιμίας (2.33) ανάγεται -κατ' ουσίαν- στην ειδική περίπτωση που περιγράψαμε στα 2.4.35 και 2.4.36, ως ακολούθως:

2.4.38 Πόρισμα. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, με* μκδ$(a, m) | b$, *η γραμμική ισοτιμία* (2.33) *διαθέτει* μκδ(a, m) *λύσεις $x \in \mathbb{Z}$ κατά μόδιο m, οι οποίες είναι τής μορφής* (2.34), *όπου x_0 η μοναδική λύση κατά μόδιο $\frac{m}{\text{μκδ}(a,m)}$ τής*

$$\left(\tfrac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\tfrac{b}{\text{μκδ}(a,m)}\right) (\mathrm{mod}\ \ \left(\tfrac{m}{\text{μκδ}(a,m)}\right)). \tag{2.36}$$

ΑΠΟΔΕΙΞΗ. Θέτοντας $\widetilde{a} := \frac{a}{\text{μκδ}(a,m)}$, $\widetilde{b} := \frac{b}{\text{μκδ}(a,m)}$ και $\widetilde{m} := \frac{m}{\text{μκδ}(a,m)}$, έχουμε μκδ$(\widetilde{a}, \widetilde{m}) = 1$ (βλ. 2.2.11 (ii)), καθώς και τις ακόλουθες αμφίπλευρες συνεπαγωγές:

$$\begin{aligned} ax \equiv b\ (\mathrm{mod}\ m) &\iff \text{μκδ}\,(a,m)\,\widetilde{a}x \equiv \text{μκδ}\,(a,m)\,\widetilde{b}\ (\mathrm{mod}\,\text{μκδ}\,(a,m)\,\widetilde{m}) \\ &\iff \widetilde{a}x \equiv \widetilde{b}\ (\mathrm{mod}\ \widetilde{m}) \\ &\iff \left(\tfrac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\tfrac{b}{\text{μκδ}(a,m)}\right)\ (\mathrm{mod}\ \ \left(\tfrac{m}{\text{μκδ}(a,m)}\right)), \end{aligned}$$

διότι μκδ$(a, m) \neq 0$ (βλ. 2.4.5 (iv)), οπότε η (2.36) ισοδυναμεί με την (2.33). □

2.4.39 Παράδειγμα. Η γραμμική ισοτιμία

$$6x \equiv 3 (\mathrm{mod}\, 21)$$

διαθέτει μκδ$(6, 21) = 3$ λύσεις κατά μόδιο 21 τής μορφής $x_0, x_0 + 7, x_0 + 14$, όπου σύμφωνα με το πόρισμα 2.4.38 το x_0 είναι η μοναδική λύση τής $2x \equiv 1 (\mathrm{mod}\, 7)$ κατά μόδιο 7. Εφαρμόζοντας τον τύπο (2.35) θέτουμε

$$x_0 = 2^{\varphi(7)-1} = 2^5 = 32 \equiv 4 (\mathrm{mod}\, 7).$$

Άρα οι λύσεις τής αρχικής είναι οι $4, 11, 18$ κατά μόδιο 21.

Κλείνουμε το παρόν κεφάλαιο παραθέτοντας μια απλή ικανή και αναγκαία συνθήκη, ούτως ώστε ένας ακέραιος > 1 να είναι *πρώτος*.

2.4.40 Θεώρημα. (Wilson) *Ένας ακέραιος $p > 1$ είναι πρώτος εάν και μόνον εάν*[16]

$$\boxed{(p-1)! \equiv -1 \pmod{p}\,.} \tag{2.37}$$

ΑΠΟΔΕΙΞΗ. Έστω p ένας πρώτος αριθμός. Εάν $p = 2$ ή $p = 3$, τότε η (2.37) είναι προφανώς αληθής. Εάν ο p είναι πρώτος ≥ 5, θεωρούμε ένα $a \in \{1, 2, \ldots, p-1\}$ και τη γραμμική ισοτιμία $ax \equiv 1 \pmod{p}$. Επειδή μκδ$(a, p) = 1$, η εν λόγω ισοτιμία έχει μοναδική λύση κατά μόδιο p, οπότε υπάρχει μονοσημάντως ορισμένος ακέραιος a', για τον οποίο ισχύει $0 \leq a' \leq p-1$ και $aa' \equiv 1 \pmod{p}$. Επειδή ο p είναι πρώτος, έχουμε

$$a = a' \Longleftrightarrow (\text{είτε } \ a = 1 \ \text{ είτε } \ a = p-1)\,. \tag{2.38}$$

Πράγματι· από την ισοτιμία $a^2 \equiv 1 \pmod{p}$ συνάγουμε ότι

$$p \mid (a-1)(a+1) \Longrightarrow (\text{είτε } \ p \mid a-1 \ \text{ είτε } \ p \mid a+1)\,,$$

απ' όπου προκύπτει η συνεπαγωγή "$\Longrightarrow$" τής (2.38), αφού έχουμε $1 \leq a \leq p-1$ και $1 \leq a' \leq p-1$. Και αντιστρόφως· εάν $a = 1$, τότε

$$\left.\begin{array}{r} a' \equiv 1 \pmod{p} \Longrightarrow p \mid a'-1 \\ 1 \leq a' \leq p-1 \end{array}\right\} \underset{\text{(βλ. 2.1.5 (ii))}}{\Longrightarrow} a'-1 = 0 \Longrightarrow a' = 1,$$

και εάν $a = p-1$, τότε

$$(p-1)\,a' \equiv 1 \pmod{p} \Longrightarrow pa' \equiv a'+1 \pmod{p}\,,$$

οπότε

$$\left.\begin{array}{r} pa' \equiv a'+1 \pmod{p} \\ pa' \equiv p \pmod{p} \end{array}\right\} \Longrightarrow p \equiv a'+1 \pmod{p}\,,$$

και, ως εκ τούτου,

$$\left.\begin{array}{r} p \equiv a'+1 \pmod{p} \Longrightarrow p \mid p-(a'+1) \\ 0 \leq p-(a'+1) \leq p-2 \end{array}\right\} \underset{\text{(βλ. 2.1.5 (ii))}}{\Longrightarrow} a' = p-1,$$

και η συνεπαγωγή "$\Longleftarrow$" τής (2.38) είναι όντως αληθής. Ομαδοποιούμε, εν συνεχεία, τους εναπομένοντες φυσικούς αριθμούς

$$\{1, 2, \ldots, p-1\} \setminus \{1, p-1\} = \{2, 3, \ldots, p-2\}$$

[16] Ο John Wilson (1741-1793) υπήρξε μαθητής τού Edward Waring (1734-1798), αλλά εγκατέλειψε αρκετά σύντομα τα Μαθηματικά. Υπηρέτησε ως δικαστικός και κατόπιν (περί το 1786) έλαβε και τον τίτλο τού ιππότη. Στο σύγγραμμά του με τον τίτλο *Meditationes algebraicae* (που δημοσιεύθηκε το 1770) ο Waring διατείνεται ότι ο Wilson είχε *εικάσει* την ισχύ τής ισοτιμίας (2.37). Ωστόσο, ο Wilson δεν μπόρεσε να την αποδείξει και πιθανώς να αρκέσθηκε σε κάποια απλά παραδείγματα. Ο Leibnitz (1646-1716) είχε επίσης εικάσει την ισχύ αυτής τής ισοτιμίας (και μάλιστα πριν το 1683), χωρίς όμως να έχει καταφέρει να την αποδείξει. Ο Lagrange (1736-1813), ορμώμενος από όσα ανέφερε ο Waring στο *Meditationes algebraicae*, εργάσθηκε σκληρά επί τού προβλήματος και τελικώς έδωσε μια ορθή απόδειξη το 1771.

κατά ζεύγη (a, a'), για τα οποία ισχύει $a \neq a'$ και $aa' \equiv 1 \pmod{p}$. Πολλαπλασιάζοντας κατά μέλη τις κατ' αυτόν τον τρόπο σχηματιζόμενες $\frac{p-3}{2}$ ισοτιμίες λαμβάνουμε

$$2 \cdot 3 \cdot \cdots (p-2) \equiv 1 \pmod{p} \Longrightarrow (p-1)! \equiv p-1 \pmod{p}.$$

Επειδή $p - 1 \equiv -1 \pmod{p}$, η (2.37) προκύπτει από το 2.1.5 (v).

Αντιστρόφως τώρα· υποθέτοντας ότι

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

για κάποιον *σύνθετο* φυσικό αριθμό $n \geq 2$, θα υπάρχει κάποιος διαιρέτης n' τού n με $1 < n' < n$, οπότε $n' \mid (n-1)!$. Επειδή

$$\left.\begin{array}{r} n' \mid n \\ n \mid (n-1)!+1 \end{array}\right\} \Longrightarrow n' \mid (n-1)!+1,$$

ο n' θα διαιρεί και τη διαφορά $(n-1)! + 1 - (n-1)! = 1$, οπότε $n' = 1$, πράγμα άτοπο. Συνεπώς ο n οφείλει να είναι *πρώτος* προκειμένου να πληροί την ως άνω ισοτιμία. □

2.4.41 Πόρισμα. *Έστω p ένας περιττός πρώτος. Τότε*

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

ΑΠΟΔΕΙΞΗ. Υποθέτοντας ότι $p \equiv 1 \pmod{4}$, θα υπάρχει ένας ακέραιος k, ούτως ώστε να ισχύει η ισότητα: $p = 4k + 1$. Επομένως,

$$\tfrac{p-1}{2} = 2k \Longrightarrow \left(\tfrac{p-1}{2}\right)! = 1 \cdot 2 \cdot \cdots \tfrac{p-1}{2} = (-1)\,(-2) \cdot \cdots \left(-\tfrac{p-1}{2}\right) \tag{2.39}$$

(προφανώς με άρτιο πλήθος εμφανιζομένων σημείων τού «μείον» στο δεξιό μέλος) και

$$\left.\begin{array}{r} -1 \equiv (p-1) (\mathrm{mod}\, p) \\ -2 \equiv (p-2) (\mathrm{mod}\, p) \\ \vdots \\ -\frac{p-1}{2} \equiv (\frac{p+1}{2}) (\mathrm{mod}\, p) \end{array}\right\} \Longrightarrow \left(\tfrac{p-1}{2}\right)! \equiv (p-1)\,(p-2) \cdots (\tfrac{p+1}{2}) (\mathrm{mod}\, p). \tag{2.40}$$

Συνδυάζοντας τις (2.39) και (2.40) λαμβάνουμε

$$\begin{aligned} \left[\left(\tfrac{p-1}{2}\right)!\right]^2 &\equiv 1 \cdot 2 \cdot \cdots (\tfrac{p-1}{2})(\tfrac{p+1}{2}) \cdots (p-2)\,(p-1) \pmod{p} \\ &\equiv (p-1)! \,(\mathrm{mod}\, p). \end{aligned}$$

Από το θεώρημα 2.4.40 τού Wilson, $(p-1)! \equiv -1 \pmod{p}$, οπότε

$$\left[\left(\tfrac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p},$$

λόγω τού (v) τής προτάσεως 2.1.5. Εν συνεχεία, ας υποθέσουμε ότι $p \equiv 1 \pmod{4}$. Τότε θα υπάρχει ένας ακέραιος k, ούτως ώστε να ισχύει η ισότητα: $p = 4k+3$. Επομένως,

$$\begin{aligned} \tfrac{p-1}{2} = 2k+1 \Longrightarrow \quad -\left(\tfrac{p-1}{2}\right)! = -1 \cdot 2 \cdot \cdots \cdot \tfrac{p-1}{2} \quad &= (-1)(-2)\cdots\left(-\tfrac{p-1}{2}\right) \\ &\equiv (p-1)\cdots\left(\tfrac{p+1}{2}\right) (\mathrm{mod}\, p), \end{aligned}$$

οπότε

$$-\left[\left(\tfrac{p-1}{2}\right)!\right]^2 \equiv 1 \cdot 2 \cdot \cdots \cdot \left(\tfrac{p-1}{2}\right)\left(\tfrac{p+1}{2}\right)\cdots(p-1) \equiv (p-1)! \equiv -1 \pmod{p},$$

εκ νέου κατόπιν εφαρμογής τού θεωρήματος 2.4.40 τού Wilson. □