Παράρτημα Β

Υπομνήσεις από τη Στοιχειώδη Θεωρία Αριθμών

Σκοπός τού παρόντος παραρτήματος είναι η υπενθύμιση κάποιων αποτελεσμάτων τής Στοιχειώδους Θεωρίας Αριθμών, ορισμένα εκ των οποίων είναι ήδη γνωστά από το σχολείο (και τα λοιπά από προηγηθείσες παραδόσεις άλλων συναφών εισαγωγικών μαθημάτων) και χρησιμοποιούνται κατ' επανάληψη στο κυρίως κείμενο. 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 ≥ 2 ως γινομένου πρώτων αριθμών, το θεώρημα τού Euler περί ισοτιμίων και η περιγραφή των λύσεων γραμμικών ισοτιμιών με έναν άγνωστο.

Β.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).

Β.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** (ακριβώς) **τον** b και ότι ο b **είναι διαιρέσιμος διά τού** a ή -ισοδυνάμως- ότι ο b είναι **πολλαπλάσιο τού** a και ότι ο a είναι **διαιρέτης** ή **παράγοντας** τού b. Για να δηλούμε ότι ο a διαιρεί τον b γράφουμε $a \mid b$, ενώ για να δηλούμε ότι ο a δεν διαιρεί τον b γράφουμε $a \nmid b$.

Β.1.2 Παράδειγμα. Οι *άρτιοι* (και αντιστοίχως, οι *περιττοί*) ακέραιοι αριθμοί εί-

ναι εξ ορισμού εκείνοι οι ακέραιοι αριθμοί οι οποίοι είναι διαιρέσιμοι (και αντιστοίχως, δεν είναι διαιρέσιμοι) διά τού 2.

Β.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* $0 \mid b$, *για κάποιον* $b \in \mathbb{Z}$, *τότε* $b = 0$.

(iv) *Εάν* $b \mid \pm 1$, *για κάποιον* $b \in \mathbb{Z}$, *τότε* $b = \pm 1$.

(v) $a \mid a$ *για κάθε* $a \in \mathbb{Z}$.

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 $\pm 1 = bc$ για κάποιον $c \in \mathbb{Z}$, οπότε κατ' ανάγκην έχουμε $(b, c) \in \{(\pm 1, \pm 1), (\pm 1, \mp 1)\}$.

(v) Προφανώς, $a = a \cdot 1$ για κάθε $a \in \mathbb{Z}$. □

Β.1.4 Σημείωση. Σε ό,τι ακολουθεί σημειώνουμε ως $|a| = \text{sign}(a)\, a$ την *απόλυτη τιμή* ενός ακεραίου a (όπου $\text{sign}(a) := 1$, όταν $a \geq 0$ και $\text{sign}(a) := -1$, όταν $a < 0$).

Β.1.5 Πρόταση. *Εάν* $a, b, c, d \in \mathbb{Z}$, *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*[1] $a \mid b$ *και* $a \mid c$, *τότε* $a \mid bx + cy$ *για κάθε* $x, y \in \mathbb{Z}$.

ΑΠΟΔΕΙΞΗ. (i) Προφανές επί τη βάσει τού ορισμού Β.1.1.

(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. Β.1.3 (iii)). Παρομοίως εάν $b = 0$, τότε από την $b \mid a$ λαμβάνουμε $a = 0$. Άρα σε κάθε περίπτωση $|a| = |b|$.

(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,

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

[1] 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 $x_1, \ldots, x_n \in \mathbb{Z}$.

(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 $x, y \in \mathbb{Z}$. □

Β.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*

$$\boxed{a = qb + r, \text{ όπου } 0 \le r < |b|\,.} \tag{Β.1}$$

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

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

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

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

δεδομένου -εξ υποθέσεως- ότι $|b| \ge 1$. Ως εκ τούτου, το S διαθέτει ένα ελάχιστο στοιχείο[2] $r \ge 0$. 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

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

ήτοι ότι $r - |b| \in S$, κάτι το οποίο θα αντέφασκε προς την επιλογή τού r. Κατά συνέπειαν, οι ανισότητες $0 \le r < |b|$ είναι όντως αληθείς. Απομένει λοιπόν να δείξουμε ότι το ανωτέρω ζεύγος (q, r) που ικανοποιεί την (Β.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 $0 \le r, r' < |b|$. Τότε

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

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

Β.1.7 Ορισμός. Τα q και r τής ταυτότητας (Β.1) ονομάζονται το **πηλίκο** και, αντιστοίχως, το **υπόλοιπο** τής **διαιρέσεως τού** a **διά τού** b. Σημειωτέον ότι το b διαιρεί (ακριβώς) το a, δηλαδή $b \mid a$, εάν και μόνον εάν $r = 0$.

[2] Κατά την «αρχή τής καλής διατάξεως», κάθε μη κενό υποσύνολο τού $\mathbb{N}$ ή τού $\mathbb{N}_0$ διαθέτει ελάχιστο στοιχείο.

► **Παράσταση φυσικού αριθμού σε μια κλίμακα**. Η εξοικείωση με την παράσταση ενός φυσικού αριθμού στο *δεκαδικό σύστημα* (στην «κλίμακα τού 10») λαμβάνει χώρα στα αρχικά στάδια τής πρωτοβάθμιας εκπαιδεύσεως. Το θεώρημα Β.1.9 μας πληροφορεί ότι, αντί τού 10, είναι δυνατόν να χρησιμοποιηθεί και οιοσδήποτε άλλος ακέραιος ≥ 2.

Β.1.8 Λήμμα. *Έστω* $s \in \mathbb{N}$, $s \geq 2$. *Εάν* $n \in \mathbb{N}_0$ *και ισχύει η ισότητα*

$$b_n s^n + b_{n-1} s^{n-1} + \cdots + b_1 s + b_0 = 0, \tag{B.2}$$

όπου $b_i \in \mathbb{Z}$ *και* $|b_i| \leq s-1$, $\forall i \in \{0,1,...,n\}$, *τότε* $b_i = 0$, $\forall i \in \{0,1,...,n\}$.

ΑΠΟΔΕΙΞΗ. Η (Β.2) γράφεται ως $b_0 = k_0 s$, όπου $k_0 := -(b_n s^{n-1} + \cdots + b_1)$. Άρα είτε $|b_0| \geq s$ είτε $k_0 = 0$. Το πρώτο ενδεχόμενο αποκλείεται από την υπόθεσή μας. Επομένως,

$$\left.\begin{array}{r} k_0 = 0 \Rightarrow b_0 = 0 \\ s \neq 0 \end{array}\right\} \underset{\text{(B.2)}}{\Longrightarrow} b_n s^{n-1} + b_{n-1} s^{n-2} + \cdots + b_1 = 0.$$

Επαναλαμβάνοντας τον ίδιο συλλογισμό συμπεραίνουμε ότι $b_1 = 0$. Συνεχίζοντας αυτήν τη διαδικασία καταλήγουμε (ύστερα από n βήματα) στο ότι ισχύουν οι ισότητες $b_0 = b_1 = \cdots = b_n = 0$. □

Β.1.9 Θεώρημα. *Εάν* $s \in \mathbb{N}$, $s \geq 2$, *τότε κάθε* $a \in \mathbb{N}$ *μπορεί να γραφεί μονοσημάντως υπό τη μορφή*

$$\boxed{a = c_n s^n + c_{n-1} s^{n-1} + \cdots + c_1 s + c_0,} \tag{B.3}$$

όπου[3] $n \in \mathbb{N}_0$, $c_i \in \{0,1,...,s-1\}$ *για κάθε* $i \in \{0,...,n-1\}$ *και* $c_n \in \{1,...,s-1\}$.

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς, κάνοντας χρήση τής μαθηματικής επαγωγής (δεύτερης μορφής), θα δείξουμε ότι κάθε $a \in \mathbb{N}$ διαθέτει μια τέτοιου είδους παράσταση. Εάν $a = 1$, τότε η $a = 1$ είναι μια παράσταση τής μορφής (Β.3) θέτοντας $n := 0$ και $c_0 := 1$. Εάν $a < s$, τότε η $a = a$ είναι μια τέτοιου είδους παράσταση, εάν θέσουμε $n := 0$ και $c_0 := a$. Εάν $a \geq s$, υποθέτουμε ότι κάθε φυσικός αριθμός $< a$ διαθέτει μια παράσταση τής μορφής (Β.3) και γράφουμε τον a (μέσω τής (Β.1)) ως $a = qs + r$, όπου $(q,r) \in \mathbb{Z} \times \mathbb{Z}$ και $q > 0$, $r \in \{0,1,...,s-1\}$ (διότι $a \geq s$). Επειδή $q < a$, το q διαθέτει (λόγω τής επαγωγικής μας υποθέσεως) μια παράσταση τής μορφής

$$q = d_m s^m + d_{m-1} s^{m-1} + \cdots + d_1 s + d_0,$$

όπου $m \in \mathbb{N}_0$, $d_j \in \{0,1,...,s-1\}$ για κάθε $j \in \{0,...,m-1\}$ και $d_m \in \{1,...,s-1\}$. Άρα

$$a = qs + r = c_n s^n + c_{n-1} s^{n-1} + \cdots + c_1 s + c_0,$$

όπου $n := m+1$, $c_i := d_{i-1}$ για κάθε $i \in \{1,...,n\}$ και $c_0 := r$.

[3] Επειδή $s^n \leq c_n s^n \leq a$, έχουμε $n \leq \frac{\ln(a)}{\ln(s)}$.

Εν συνεχεία, θα αποδείξουμε τη *μοναδικότητα* τής παραστάσεως (Β.3) τού a. Ας υποθέσουμε ότι ο a, πέραν τής (Β.3), έχει και την παράσταση

$$a = c'_k s^k + c'_{k-1} s^{n-1} + \cdots + c'_1 s + c'_0, \tag{Β.4}$$

όπου $k \in \mathbb{N}_0$, $c'_\varrho \in \{0, 1, ..., s-1\}$ για κάθε $\varrho \in \{0, ..., k-1\}$ και $c'_k \in \{1, ..., s-1\}$. Εάν $k > n$, τότε οι (Β.3) και (Β.4) δίδουν

$$c'_k s^k + \cdots + c'_{n+1} s^{n+1} + (c'_n - c_n)\, s^n + \cdots + (c'_1 - c_1)\, s + (c'_0 - c_0) = 0. \tag{Β.5}$$

Επειδή $|c'_i - c_i| \leq s-1, \forall i \in \{0, 1, ..., n\}$, το λήμμα Β.1.8 μας πληροφορεί ότι όλοι οι συντελεστές τού αριστερού μέλους τής (Β.5) είναι ίσοι με το 0. Τούτο όμως είναι άτοπο, διότι $c'_k > 0$. Άρα δεν μπορεί να ισχύει η ανισότητα $k > n$. Παρομοίως (με εναλλαγή των ρόλων των k και n) αποδεικνύουμε ότι δεν μπορεί να ισχύει ούτε η ανισότητα $k < n$. Κατά συνέπειαν, $k = n$ και

$$(c'_n - c_n)\, s^n + \cdots + (c'_1 - c_1)\, s + (c'_0 - c_0) = 0,$$

οπότε από το λήμμα Β.1.8 έπεται ότι $c'_i = c_i, \forall i \in \{0, 1, ..., n\}$. □

Β.1.10 Ορισμός. Η παράσταση (Β.3) καλείται **παράσταση τού a στην κλίμακα τού s** (και ο s **βάση τής κλίμακας**).

Β.1.11 Συμβολισμός. Εάν ένας $a \in \mathbb{N}$ έχει στην κλίμακα τού s την παράσταση (Β.3), τότε συνήθως γράφουμε εν συντομία

$$\boxed{a = (c_n c_{n-1} ... c_1 c_0)_s.}$$

Β.1.12 Παραδείγματα. (i) Για τον $a = 456$ έχουμε προφανώς

$$456 = (456)_{10} = 4 \cdot 10^2 + 5 \cdot 10 + 6 = 7 \cdot 8^2 + 1 \cdot 8 + 0 = (710)_8.$$

(ii) Ο φυσικός αριθμός $a = 375$ στην κλίμακα τού 2 (ήτοι *στο δυαδικό σύστημα*) γράφεται ως $(101110111)_2$.

Β.2 ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ ΚΑΙ ΕΛΑΧΙΣΤΟ ΚΟΙΝΟ ΠΟΛΛΑΠΛΑΣΙΟ

Β.2.1 Ορισμός. Εάν $n \in \mathbb{N},\ n \geq 2$, και εάν οι $a_1, ..., a_n$ είναι ακέραιοι με έναν τουλάχιστον εξ αυτών $\neq 0$, τότε κάθε ακέραιος που διαιρεί καθέναν εκ των $a_1, ..., a_n$ καλείται **κοινός διαιρέτης** των $a_1, ..., a_n$. Έστω S το σύνολο των θετικών κοινών διαιρετών των $a_1, ..., a_n$. 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, $\delta \leq |a_k|, \forall \delta \in S$. Κατά συνέπειαν, το S είναι πεπερασμένο. Το μέγιστο στοιχείο τού συνόλου S (ως προς την " $\leq$ ") καλείται **μέγιστος κοινός διαιρέτης** των $a_1, ..., a_n$ και συμβολίζεται ως

μκδ$(a_1,...,a_n)$. 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,

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

δηλαδή ο μέγιστος κοινός διαιρέτης των $a_1,...,a_n$ είναι *ανεξάρτητος* των προσήμων τους. Επίσης, επειδή κάθε ακέραιος διαιρεί το μηδέν, έχουμε

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

και, ειδικότερα[4], μκδ$(0, a) =$ μκδ$(a, 0) = 0$, $\forall a \in \mathbb{Z}\setminus\{0\}$. (Γι' αυτόν τον λόγο μπορούμε εφεξής να υποθέτουμε ότι κανείς εκ των εκάστοτε θεωρουμένων ακεραίων $a_1,..., a_n$ δεν είναι μηδέν.)

Β.2.2 Ορισμός. Δυο μη μηδενικοί 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).

Β.2.3 Ορισμός. Εάν $n \in \mathbb{N},\ n \geq 2$, και $a_1,..., a_n \in \mathbb{Z}\setminus\{0\}$ με μκδ$(a_1,..., a_n) = 1$, τότε λέμε ότι οι $a_1,..., a_n$ 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 $a_1,..., a_n$ είναι **ανά δύο (ή ανά ζεύγη) σχετικώς πρώτοι** ή, εναλλακτικώς, ότι είναι **ανά δύο (ή ανά ζεύγη) πρώτοι μεταξύ τους**.

Β.2.4 Παρατήρηση. Εάν οι $a_1,..., a_n$ είναι ανά δύο σχετικώς πρώτοι, τότε είναι και σχετικώς πρώτοι (ως ολότητα). Αντιθέτως, το να είναι οι ακέραιοι $a_1,..., a_n$ σχετικώς πρώτοι δεν σημαίνει ότι αυτοί είναι κατ' ανάγκην και ανά δύο σχετικώς πρώτοι. Π.χ., μκδ$(5, 6, 10) = 1$, με μκδ$(5, 6) = 1$, αλλά μκδ$(5, 10) = 5$ και μκδ$(6, 10) = 2$.

Β.2.5 Θεώρημα. *Εάν* $n \in \mathbb{N},\ n \geq 2,\ a_1,..., a_n \in \mathbb{Z}\setminus\{0\}$ *και* $d :=$ μκδ$(a_1,..., a_n)$, *τότε υπάρχουν* $k_1,..., k_n \in \mathbb{Z}$, *τέτοιοι ώστε να ισχύει η ισότητα*[5]

$$\boxed{d = k_1a_1 + \cdots + k_na_n.} \tag{Β.6}$$

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

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

για κάθε $j, l \in \{1,..., n\}$, έχουμε προφανώς $a_l = \sum_{j=1}^{n} \varepsilon_{j,l} a_j \in S,\ \forall l \in \{1,..., n\}$. Εάν κάποιος εκ των $a_1,..., a_n$ είναι > 0, τότε $S \cap \mathbb{N} \neq \varnothing$. Ωστόσο, το ότι $S \cap \mathbb{N} \neq \varnothing$ είναι

[4] *Σύμβαση*: Ακόμη και όταν $a = 0$, θέτουμε μκδ$(0, 0) := 0$.

[5] Είθισται να λέμε ότι μέσω τής (Β.6) ο d εκφράζεται ως *ακέραιος γραμμικός συνδυασμός* των $a_1,..., a_n$ (με *συντελεστές* του τους $k_1,..., k_n$).

πάντοτε αληθές, διότι ακόμη και εάν $a_l < 0$ για *κάθε* $l \in \{1,...,n\}$, 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 (καθώς το $\mathbb{N}$ είναι καλώς διατεταγμένο), 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 Β.1.6) ένα μονοσημάντως ορισμένο ζεύγος $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, ούτως ώστε να ισχύει

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

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 $j \in \{1,...,n\}$. Επιπροσθέτως, για οιονδήποτε $\delta \in \mathbb{N}$, για τον οποίο ισχύει $\delta \mid a_1,...,\ \delta \mid a_n$, έχουμε

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

(βλ. Β.1.5 (vi) και (ii)), οπότε τελικώς $d' = d$. □

Β.2.6 Πόρισμα. *Εάν* $n \in \mathbb{N},\ n \geq 2$, *και* $a_1,..., a_n \in \mathbb{Z} \setminus \{0\}$, *τότε ένας* $d \in \mathbb{N}$ *ισούται με τον* μκδ$(a_1,..., a_n)$ *εάν και μόνον εάν ισχύουν τα ακόλουθα*:

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

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

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το θεώρημα Β.2.5 υπάρχουν $k_1,..., k_n \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα μκδ$(a_1,..., a_n) = k_1 a_1 + \cdots + k_n a_n$. Το (i) ισχύει εξ ορισμού. Για την απόδειξη τού (ii) αρκεί να θεωρήσουμε τυχόντα θετικό κοινό διαιρέτη δ των $a_1,..., a_n$ και να αποδείξουμε ότι αυτός διαιρεί τον μέγιστο κοινό διαιρέτη τους. Επειδή $\delta \mid a_j \Longrightarrow \delta \mid k_j a_j,\ \forall j \in \{1,...,n\}$, διαπιστώνουμε πράγματι ότι $\delta \mid$μκδ$(a_1,..., a_n)$ (πρβλ. Β.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 $a_1,..., a_n$ (λόγω τού (i)) και *οιοσδήποτε* θετικός κοινός διαιρέτης δ των $a_1,..., a_n$ διαιρεί τον d (λόγω τού (ii)), οπότε $\delta \leq d$ (βλ. Β.1.5 (ii)). Επομένως, $d =$ μκδ$(a_1,..., a_n)$. □

Β.2.7 Πόρισμα. *Έστω ότι* $n \in \mathbb{N},\ n \geq 2$, *και ότι οι* $a_1,..., a_n \in \mathbb{Z} \setminus \{0\}$. *Εάν ο* d *είναι ένας θετικός κοινός διαιρέτης των* $a_1,..., a_n$, *ο οποίος γράφεται υπό τη μορφή* $d = k_1 a_1 + \cdots + k_n a_n,\ k_1,..., k_n \in \mathbb{Z}$, *τότε* $d =$ μκδ$(a_1,..., a_n)$.

ΑΠΟΔΕΙΞΗ. Εάν δ είναι ένας θετικός κοινός διαιρέτης των $a_1,..., a_n$, τότε

$$\delta \mid a_j \Rightarrow [\delta \mid k_j a_j,\ \forall j \in \{1,...,n\}] \Rightarrow \delta \mid d.$$

(Βλ. Β.1.5 (vi).) Άρα $d =$ μκδ$(a_1,..., a_n)$ βάσει τού πορίσματος Β.2.7. □

Β.2.8 Πόρισμα. *Εάν* $n \in \mathbb{N},\ n \geq 2$, *και* $a_1,...,a_n \in \mathbb{Z}\setminus\{0\}$, *τότε οι* $a_1,...,a_n$ *είναι πρώτοι μεταξύ τους εάν και μόνον εάν υπάρχουν* $k_1,...,k_n \in \mathbb{Z}$, *τέτοιοι ώστε να ισχύει η ισότητα*

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

ΑΠΟΔΕΙΞΗ. Εάν οι $a_1,...,a_n$ είναι πρώτοι μεταξύ τους, τότε η ως άνω ισότητα είναι προφανής από το θεώρημα Β.2.5. Εάν, αντιστρόφως, $k_1a_1 + \cdots + k_na_n = 1$ για κάποιους ακεραίους $k_1,...,k_n$, έχουμε $1 \mid a_j$ για κάθε $j \in \{1,...,n\}$, οπότε μκδ$(a_1,...,a_n) = 1$ δυνάμει τού πορίσματος Β.2.7. □

Β.2.9 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 Β.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 $a \mid c$ (βλ. Β.1.5(vi)). □

Β.2.10 Πόρισμα. *Εάν* $a, b, c \in \mathbb{Z}\setminus\{0\}$, *τότε ισχύει η συνεπαγωγή*

$$[\text{μκδ}(a, b) = 1,\ a \mid c \ \text{ και } \ b \mid c] \Longrightarrow ab \mid c.$$

ΑΠΟΔΕΙΞΗ. Επειδή μκδ$(a, b) = 1$, βάσει τού Β.2.8 υπάρχουν $k, l \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα $ka + lb = 1$. Επομένως,

$$[c = kac + lbc,\ ab \mid ac \ \text{ και } \ ab \mid bc] \Longrightarrow ab \mid c$$

λόγω των (iv) και (vi) τής προτάσεως Β.1.5. □

Β.2.11 Πόρισμα. *Εάν* $a, b \in \mathbb{N}$ *με* μκδ$(a, b) = 1$, *τότε υπάρχουν* $\kappa, \lambda \in \mathbb{N}$, *τέτοιοι ώστε να ισχύει* $\kappa a - \lambda b = 1$.

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το πόρισμα Β.2.8 υπάρχουν $k, l \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα $ka + lb = 1$. Επιλέγουμε έναν ακέραιο αριθμό t με $t > -\frac{k}{b}$ και $t > \frac{l}{a}$, και θέτουμε $\kappa := k + bt$ και $\lambda := -(l - at)$. Προφανώς, $\kappa \geq 1$, $\lambda \geq 1$, και $\kappa a - \lambda b = ka + lb = 1$. □

Β.2.12 Πόρισμα. *Εάν* $a, b, c \in \mathbb{Z}\setminus\{0\}$, *τότε*

$$\text{μκδ}(a, bc) = 1 \Longleftrightarrow [\text{μκδ}(a, b) = 1 \text{ και μκδ}(a, c) = 1.]$$

ΑΠΟΔΕΙΞΗ. Εάν μκδ$(a, bc) = 1$, τότε κατά το πόρισμα Β.2.8 υπάρχουν $k, l \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα $ka + lbc = 1$. Με εκ νέου εφαρμογή τού πορίσματος Β.2.8 (και, συγκεκριμένα, τής αντίστροφης συνεπαγωγής που δηλοί το «μόνον εάν») συμπεραίνουμε ότι μκδ$(a, b) = 1$ και μκδ$(a, c) = 1$. Και αντιστρόφως· υποθέτοντας ότι μκδ$(a, b) = 1$ και μκδ$(a, c) = 1$, θα υπάρχουν $r, s, t, u \in \mathbb{Z}$, τέτοιοι ώστε

$$\left.\begin{aligned} ra + sb &= 1 \\ ta + uc &= 1 \end{aligned}\right\} \Longrightarrow ra + sb\,(ta + uc) = 1 = (r + stb)\,a + (su)bc,$$

οπότε και πάλι μέσω τού Β.2.8 προκύπτει ότι μκδ$(a, bc) = 1$. □

Β.2.13 Πόρισμα. *Εάν* $a, b \in \mathbb{Z}\setminus\{0\}$ *με* μκδ$(a,b)=1$, *τότε* μκδ$(a^m, b^n)=1$ *για κάθε ζεύγος* $(m,n)\in\mathbb{N}\times\mathbb{N}$.

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. Υποθέτουμε ότι $m=1$. Θα αποδείξουμε μέσω μαθηματικής επαγωγής ως προς τον n ότι μκδ$(a,b^n)=1$. Για $n=1$ αυτή η ισότητα είναι (εξ υποθέσεως) αληθής. Εάν υποθέσουμε ότι $n\geq 2$ και ότι μκδ$(a,b^{n-1})=1$, τότε

$$\left[\text{μκδ}(a,b)=1 \text{ και } \text{μκδ}(a,b^{n-1})=1\right] \underset{\text{Β.2.12}}{\Longrightarrow} \text{μκδ}(a,b^n)=1.$$

Βήμα 2ο. Θα αποδείξουμε μέσω μαθηματικής επαγωγής ως προς τον m ότι μκδ$(a^m,b^n)=1$. Για $m=1$ η εν λόγω ισότητα είναι αληθής (βάσει των προαναφερθέντων στο 1ο βήμα). Εάν υποθέσουμε ότι $m\geq 2$ και ότι μκδ$(a^{m-1},b^n)=1$, τότε $\left[\text{μκδ}(a,b^n)=1 \text{ και } \text{μκδ}(a^{m-1},b^n)=1\right] \underset{\text{Β.2.12}}{\Longrightarrow} \text{μκδ}(a^m,b^n)=1$. □

Β.2.14 Πρόταση. *Εάν* $n\in\mathbb{N},\ n\geq 2$, *και εάν οι* $\lambda, a_1,...,a_n$ *είναι μη μηδενικοί ακέραιοι, τότε ισχύουν τα ακόλουθα*:

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

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

(iii) μκδ$(a_1,...,a_n)$ = 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$(a_1,...,a_n)=d$, τότε κατά το θεώρημα Β.2.5 υπάρχουν ακέραιοι $k_1,...,k_n$, τέτοιοι ώστε να ισχύει η ισότητα $d=k_1a_1+\cdots+k_na_n$. Επομένως, $d\,|\lambda| = \sum_{j=1}^{n} k_ja_j\,|\lambda| = \sum_{j=1}^{n} (\text{sign}\,(\lambda)\,k_j)\ a_j\lambda$, κι επειδή $d\mid a_j \Rightarrow d\,|\lambda| \mid a_j\lambda$, για κάθε $j\in\{1,...,n\}$, ο μ.κ.δ. των $\lambda a_1,...,\lambda a_n$ είναι ο $d\,|\lambda|$ δυνάμει τού πορίσματος Β.2.7.

(ii) Σύμφωνα με το (i), $d=$ μκδ$(a_1,...,a_n)=$ μκδ$(d\,\frac{a_1}{d},...,d\,\frac{a_n}{d})=d$ μκδ$(\frac{a_1}{d},...,\frac{a_n}{d})$, οπότε λαμβάνουμε μκδ$(\frac{a_1}{d},...,\frac{a_n}{d})=1$.

(iii) Κατόπιν εισαγωγής των συντομογραφιών

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

παρατηρούμε ότι $[d\mid a_j\Rightarrow d\mid \nu_ja_j, \forall j\in\{2,..,n\}]\Rightarrow d\mid a_1+\nu_2a_2+\cdots+\nu_na_n$. Κατά το πόρισμα Β.2.6, $d\mid d'$. Και αντιστρόφως· επειδή

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

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 $d'\mid a_j,\ \forall j\in\{1,2,...,n\}$, απ' όπου έπεται ότι $d'\mid d$ (βλ. Β.2.6). Επειδή $d,d'\in\mathbb{N}$, οι σχέσεις διαιρετότητας $d\mid d'$ και $d'\mid d$ δίδουν $d=d'$ (βλ. Β.1.5 (iii)). □

Β.2.15 Πόρισμα. *Εάν* $m,n\in\mathbb{N}$ *και* $a\in\mathbb{N}, a\geq 2$, *τότε*

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

ΑΠΟΔΕΙΞΗ. Θέτοντας $d := \text{μκδ}(a^m-1, a^n-1), \delta := \text{μκδ}(m,n)$ και $\mathfrak{d} := \text{μκδ}(d,a)$ παρατηρούμε εν πρώτοις ότι

$$a^m - 1 = (a^\delta)^{\frac{m}{\delta}} - 1 = (a^\delta - 1)((a^\delta)^{\frac{m}{\delta}-1} + (a^\delta)^{\frac{m}{\delta}-2} + \cdots + 1),$$

οπότε $a^\delta - 1 \mid a^m - 1$. Κατ' αναλογίαν, $a^\delta - 1 \mid a^n - 1$. Από το πόρισμα Β.2.6 έπεται ότι $a^\delta - 1 \mid d$. Εν συνεχεία, παρατηρούμε ότι $\text{μκδ}(\frac{m}{\delta}, \frac{n}{\delta}) = 1$ (βλ. Β.2.14 (ii)), οπότε (κατόπιν εφαρμογής τού πορίσματος Β.2.11) υπάρχουν $\kappa, \lambda \in \mathbb{N}$, τέτοιοι ώστε να ισχύει $\kappa\frac{m}{\delta} - \lambda\frac{n}{\delta} = 1 \Longrightarrow \kappa m - \lambda n = \delta$. Σημειωτέον ότι

$$[d \mid a^m - 1 \text{ και } a^m - 1 \mid a^{\kappa m} - 1] \underset{\text{Β.1.5 (v)}}{\Longrightarrow} d \mid a^{\kappa m} - 1$$

και, παρομοίως, $d \mid a^{\lambda n} - 1$. Εξ αυτών προκύπτει ότι

$$d \mid ((a^{\kappa m} - 1) - (a^{\lambda n} - 1)) = a^{\kappa m} - a^{\lambda n} = a^{\lambda n}(a^{\kappa m - \lambda n} - 1) = a^{\lambda n}(a^\delta - 1).$$

(Βλ. Β.1.5 (vi).) Επειδή $\mathfrak{d} \mid a \Rightarrow \mathfrak{d} \mid a^m$ και $[\mathfrak{d} \mid d \text{ και } d \mid a^m - 1] \underset{\text{Β.1.5 (v)}}{\Longrightarrow} \mathfrak{d} \mid a^m - 1$, έχουμε $\mathfrak{d} \mid a^m - (a^m - 1) = 1 \Rightarrow \mathfrak{d} = 1$ και

$$\left.\begin{array}{r} d \mid a^{\lambda n}(a^\delta - 1) \\ \mathfrak{d} = \text{μκδ}(d,a) = 1 \underset{\text{Β.2.13}}{\Longrightarrow} \text{μκδ}(d, a^{\lambda n}) = 1 \end{array}\right\} \underset{\text{Β.2.9}}{\Longrightarrow} d \mid a^\delta - 1.$$

Άρα τελικώς, $d = a^\delta - 1$. □

Β.2.16 Πρόταση. *Εάν $n \in \mathbb{N},\ n \geq 3$, και εάν $a_1,...,a_n \in \mathbb{Z}\setminus\{0\}$, τότε για κάθε $k \in \mathbb{Z}, 1 \leq k \leq n-2$, ισχύει η ισότητα*

$$\boxed{\text{μκδ}(a_1,...,a_n) = \text{μκδ}(a_1,...,a_k,\ \text{μκδ}(a_{k+1},...,a_n)).} \tag{Β.7}$$

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

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

Επομένως, $\text{μκδ}(a_1,...,a_n) \mid a_j$ για οιονδήποτε δείκτη $j \in \{1,...,n\}$ και $\text{μκδ}(a_1,...,a_n) \mid \text{μκδ}(a_{k+1},...,a_n)$, απ' όπου συνάγεται ότι

$$\text{μκδ}(a_1,...,a_n) \mid \text{μκδ}(a_1,...,a_k, \text{μκδ}(a_{k+1},...,a_n)). \tag{Β.8}$$

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

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

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

$$\text{μκδ}(a_1,...,a_k, \text{μκδ}(a_{k+1},...,a_n)) \mid \text{μκδ}(a_1,...,a_n). \tag{Β.9}$$

Επειδή οι προκείμενοι μέγιστοι κοινοί διαιρέτες είναι > 0, από τις (Β.8), (Β.9) και το (iii) τής προτάσεως Β.1.5 συμπεραίνουμε την ισχύ τής ισότητας (Β.7). □

Β.2.17 Παρατήρηση. Θέτοντας $k=1$ και εφαρμόζοντας τον τύπο (Β.7) $n-1$ φορές είναι δυνατή η αναγωγή τής ευρέσεως τού μεγίστου κοινού διαιρέτη $n \geq 3$ μη μηδενικών ακεραίων αριθμών $a_1,...,a_n$ 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 (Β.1) ως ακολούθως: Επειδή $\text{μκδ}(a,b) = \text{μκδ}(|a|,|b|)$ μπορούμε -χωρίς βλάβη τής γενικότητας- να υποθέσουμε ότι $a \geq b > 0$. Κατά το θεώρημα Β.1.6 υπάρχουν μονοσημάντως ορισμένα ζεύγη ακεραίων αριθμών (q_j, r_j), $1 \leq j \leq n+1$, ούτως ώστε να ισχύουν οι ισότητες:

$$\begin{cases} r_0 = r_1 q_1 + r_2, & 0 \leq r_2 < r_1 \\ r_1 = r_2 q_2 + r_3, & 0 \leq r_3 < r_2 \\ r_2 = r_3 q_3 + r_4, & 0 \leq r_4 < r_3 \\ \cdots\cdots & \cdots\cdots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} = r_n q_n + r_{n+1}, & 0 \leq r_{n+1} < r_n. \end{cases} \tag{Β.10}$$

(Εάν $\exists r_j$, $j \geq 2$, με $r_j = 0$, τότε σταματούμε). Εξ αυτών συνάγεται -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* (σαφώς 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 $r_{n_*+1} = 0$.

Β.2.18 Πρόταση. (Ευκλείδειος αλγόριθμος) *Ο μέγιστος κοινός διαιρέτης των a και b είναι ο*

$$\boxed{\text{μκδ}(a,b) = r_{n_*}.} \tag{Β.11}$$

ΑΠΟΔΕΙΞΗ. Σύμφωνα με την πρόταση Β.2.14 (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 $\text{μκδ}(r_1,r_2) = \text{μκδ}(r_2,r_3) = \cdots = \text{μκδ}(r_{n_*-1}, r_{n_*}) = \text{μκδ}(r_{n_*} q_{n_*}, r_{n_*}) = r_{n_*}$, απ' όπου έπεται η ισότητα (Β.11). □

Β.2.19 Παράδειγμα. Ο μέγιστος κοινός διαιρέτης των $a = 240$ και $b = 50$, λαμβανομένου υπ' όψιν ότι $240 = 50\cdot 4 + 40$, $50 = 40\cdot 1 + 10$, $40 = 10\cdot 4 + 0$, υπολογίζεται μέσω των ισοτήτων $\text{μκδ}(240,50) = \text{μκδ}(50,40) = \text{μκδ}(40,10) = 10$.

Β.2.20 Σημείωση. Το θεώρημα Β.2.5 μας πληροφορεί ότι ο μέγιστος κοινός διαιρέτης n μη μηδενικών ακεραίων αριθμών (όπου $n \geq 2$) 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 μκδ(a, b) ως ακεραίου γραμμικού συνδυασμού των a και b, ως ακολούθως:

Β.2.21 Πρόταση. *Εάν $a, b \in \mathbb{Z}\setminus\{0\}$ και $a \geq b$, τότε*

$$\boxed{\text{μκδ}(a, b) = s_{n_*}a + t_{n_*}b,} \tag{Β.12}$$

με[6] $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$ *και* $s_j = s_{j-2} - q_{j-1}s_{j-1},\ t_j = t_{j-2} - q_{j-1}t_{j-1}$, *για κάθε* $j \in \{2,...,n_*\}$, *όπου τα* $q_1, q_2,..., q_{n_*-1}$ *είναι τα πηλίκα των διαιρέσεων* (Β.10) *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 (Β.10) θα αποδείξουμε τις ισότητες

$$r_j = s_j a + t_j b,\ \ \forall j \in \{0, 1,..., n_*\}, \tag{Β.13}$$

απ' όπου προκύπτει η (Β.12), λόγω τού ότι μκδ$(a, b) = r_{n_*}$. Αρκεί να εργασθούμε επαγωγικώς ως προς τον 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 $j \in \{1,..., k-1\}$, 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. □

Β.2.22 Παρατήρηση. (i) Χρησιμοποιώντας $n - 1$ φορές την (Β.7) (για $k = 1$, βλ. παρατήρηση Β.2.17) και την ισότητα (Β.12) είναι δυνατός ο υπολογισμός *συγκεκριμένων* συντελεστών $k_1,..., k_n \in \mathbb{Z}$ τού $d =$ μκδ$(a_1,..., a_n)$ για την έκφρασή του ως γραμμικού συνδυασμού (Β.6). Ωστόσο, θα πρέπει εδώ να τονισθεί ότι η επιλογή ακεραίων $k_1,..., k_n$, τέτοιων ώστε να ισχύει η (Β.6) δεν είναι κατά κανέναν τρόπο μονοσημάντως ορισμένη!

(ii) Για να καταστεί περισσότερο σαφές το ότι η επιλογή των ως άνω συντελεστών δεν είναι μονοσημάντως ορισμένη *ακόμη και για* $n = 2$, θεωρούμε $a, b \in \mathbb{Z}\setminus\{0\}$ και θέτουμε $d :=$ μκδ(a, b). Εάν $d = sa + tb$ για κατάλληλους $s, t \in \mathbb{Z}$, τότε

$$d = (s + k\left(\tfrac{b}{d}\right))a + (t - k\left(\tfrac{a}{d}\right))b,\ \ \forall k \in \mathbb{Z}.$$

[6] 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.

Β.2.23 Ορισμός. Έστω ότι $n \in \mathbb{N}$ και ότι οι $a_1,...,a_n$ είναι ακέραιοι αριθμοί. Ένας ακέραιος l καλείται **κοινό πολλαπλάσιο** των $a_1,..,a_n$ όταν $a_1 \mid l,..,\ a_n \mid l$. (Σημειωτέον ότι εάν ένας εκ των $a_1,...,a_n$ είναι ίσος με το 0, τότε το μοναδικό πολλαπλάσιό τους είναι το 0).

Β.2.24 Ορισμός. Έστω ότι $n \in \mathbb{N}$ και ότι $a_1,...,a_n \in \mathbb{Z}\setminus\{0\}$. Προφανώς, ο φυσικός αριθμός $|a_1 \cdots a_n|$ είναι ένα κοινό πολλαπλάσιο των $a_1,...,a_n$. Ως εκ τούτου, το σύνολο των θετικών πολλαπλασίων των $a_1,...,a_n$ είναι μη κενό και διαθέτει ένα και μόνον *ελάχιστο* στοιχείο. Το στοιχείο αυτό καλείται **ελάχιστο κοινό πολλαπλάσιο** των $a_1,...,a_n$ και συμβολίζεται ως εκπ$(a_1,...,a_n)$. Επειδή το σύνολο των θετικών πολλαπλασίων των $a_1,...,a_n$ ισούται με το σύνολο των θετικών πολλαπλασίων των $|a_1|,...,|a_n|$, συμπεραίνουμε ότι εκπ$(a_1,...,a_n) =$ εκπ$(|a_1|,...,|a_n|)$. (*Σύμβαση*: Είναι δυνατή η επέκταση τής εννοίας τού ελαχίστου κοινού πολλαπλασίου ακόμη και όταν *τουλάχιστον ένας* εκ των $a_1,...,a_n$ είναι $= 0$. Εν τοιαύτη περιπτώσει θέτουμε εκπ$(a_1,...,a_n) := 0$.)

Β.2.25 Πρόταση. *Εάν $n \in \mathbb{N}$ και εάν $a_1,...,a_n \in \mathbb{Z}\setminus\{0\}$, τότε ένας $m \in \mathbb{N}$ ισούται με το* εκπ$(a_1,...,a_n)$ *εάν και μόνον εάν ισχύουν τα ακόλουθα*:

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

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

Απόδειξη. Εάν $m =$ εκπ$(a_1,...,a_n)$, τότε εξ ορισμού $a_1 \mid m,...,\ a_n \mid m$, οπότε ισχύει το (i). Εξάλλου, για οιονδήποτε $l \in \mathbb{N}$, για τον οποίο ισχύει $a_1 \mid l,...,\ a_n \mid l$, υπάρχει (κατά το Β.1.6) ένα μονοσημάντως ορισμένο ζεύγος $(q,r) \in \mathbb{Z}\times\mathbb{Z}$, ούτως ώστε να ισχύει $l = qm + r$, όπου $0 \le r < m$. Επειδή

$$[a_1 \mid m,...,\ a_n \mid m \text{ και } a_1 \mid l,...,\ a_n \mid l] \Rightarrow a_1 \mid r,...,\ a_n \mid r,$$

το r είναι ένα κοινό πολλαπλάσιο των $a_1,...,a_n$. Άρα $r = 0$ (διότι εάν $r > 0$, θα είχαμε $r \ge m$, 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 $a_1,...,a_n$ και για οιοδήποτε κοινό πολλαπλάσιο l των $a_1,...,a_n$ έχουμε $m \mid l$, απ' όπου συμπεραίνουμε ότι $m \le l$, ήτοι ότι $m =$ εκπ$(a_1,...,a_n)$. □

Β.2.26 Πρόταση. *Εάν $n \in \mathbb{N}$ και $\lambda, a_1,...,a_n \in \mathbb{Z}\setminus\{0\}$, τότε ισχύουν τα εξής*:

(i) εκπ$(\lambda a_1,...,\lambda a_n) = |\lambda|$ εκπ$(a_1,...,a_n)$.

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

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

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

οπότε, δυνάμει τής προτάσεως Β.2.25, εκπ$(\lambda a_1,...,\lambda a_n) \mid |\lambda|\, m$. Επιπροσθέτως,

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

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

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

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

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

για κάθε $j \in \{1,..., n\}$, οπότε (λόγω τής προτάσεως Β.2.25)

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

Επειδή (λόγω τού (i))

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

λαμβάνουμε $\text{εκπ}(\frac{m}{a_1},..., \frac{m}{a_n})m \mid m$, οπότε $\text{μκδ}(\frac{m}{a_1},..., \frac{m}{a_n}) = 1$. □

Β.2.27 Πρόταση. *Εάν* $n \in \mathbb{N},\ n \geq 3$, *και εάν* $a_1,..., a_n \in \mathbb{Z}\setminus\{0\}$, *τότε για κάθε* $k \in \mathbb{Z}, 1 \leq k \leq n-2$, *ισχύει η ισότητα*:

$$\boxed{\text{εκπ}(a_1,..., a_n) = \text{εκπ}(a_1,..., a_k, \text{εκπ}(a_{k+1},..., a_n)).} \qquad \text{(Β.14)}$$

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

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

Επομένως, $a_j \mid \text{εκπ}(a_1,..., a_n), \forall j \in \{1,.., n\}$ και $\text{εκπ}(a_{k+1},..., a_n) \mid \text{εκπ}(a_1,..., a_n)$, απ' όπου συνάγεται ότι

$$\text{εκπ}(a_1,..., a_k, \text{εκπ}(a_{k+1},..., a_n)) \mid \text{εκπ}(a_1,..., a_n). \qquad \text{(Β.15)}$$

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

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

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

$$\text{εκπ}(a_1,..., a_n) \mid \text{εκπ}(a_1,..., a_k, \text{εκπ}(a_{k+1},..., a_n)). \qquad \text{(Β.16)}$$

Επειδή τα προκείμενα ελάχιστα κοινά πολλαπλάσια είναι θετικοί ακέραιοι, από τις (Β.15), (Β.16) και το (iii) τής προτάσεως Β.1.5 συμπεραίνουμε την ισχύ τής ισότητας (Β.14). □

Β.2.28 Παρατήρηση. Θέτοντας $k = 1$ και εφαρμόζοντας τον τύπο (Β.14) $n-1$ φορές είναι δυνατή η αναγωγή τής ευρέσεως τού ελαχίστου κοινού πολλαπλασίου $n \geq 3$ μη μηδενικών ακεραίων αριθμών $a_1,..., a_n$ 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 (Β.17), τον οποίο αποδεικνύουμε στην επομένη πρόταση.

Β.2.29 Πρόταση. *Για οιουσδήποτε* $a, b \in \mathbb{Z}\smallsetminus\{0\}$ *έχουμε*

$$\boxed{\text{μκδ}(a,b)\ \text{εκπ}(a,b) = |ab|\,.} \tag{Β.17}$$

ΑΠΟΔΕΙΞΗ. Επειδή $\text{μκδ}(a,b) \mid a$ και $\text{μκδ}(a,b) \mid b$, έχουμε $\text{μκδ}(a,b) \mid |ab|$. Αρκεί λοιπόν να αποδείξουμε ότι ο θετικός ακέραιος αριθμός $\frac{|ab|}{\text{μκδ}(a,b)}$ ισούται με το $\text{εκπ}(a,b)$. Προς τούτο θα χρησιμοποιήσουμε την πρόταση Β.2.25. Κατ' αρχάς, $a \mid \frac{|ab|}{\text{μκδ}(a,b)}$ και $b \mid \frac{|ab|}{\text{μκδ}(a,b)}$. Ας υποθέσουμε ότι ο l είναι ενας θετικός ακέραιος, για τον οποίο ισχύει $a \mid l$ και $b \mid l$. Κατά το θεώρημα Β.2.5, υπάρχουν ακέραιοι αριθμοί s, t, τέτοιοι ώστε να ισχύει η ισότητα: $\text{μκδ}(a,b) = sa + tb$. Συνεπώς,

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

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

► **Περί των συνδέσμων** $(\mathbb{N}, |)$, $(\mathbb{N}_0, |)$. Μέσω τής σχέσεως διαιρετότητας τα σύνολα των φυσικών και των μη αρνητικών ακεραίων καθίστανται *σύνδεσμοι*.

Β.2.30 Πρόταση. *Τα ζεύγη* $(\mathfrak{X}, |)$, *όπου* $\mathfrak{X} \in \{\mathbb{N}, \mathbb{N}_0\}$ *και* " | " *η συνήθης σχέση διαιρετότητας*[7]

$$[a \mid b \underset{\text{ορσ}}{\Longleftrightarrow} \exists c \in \mathbb{Z} : b = ac],\ \forall (a,b) \in \mathfrak{X} \times \mathfrak{X},$$

αποτελούν μερικώς (μη ολικώς) διατεταγμένα σύνολα.

ΑΠΟΔΕΙΞΗ. Η αυτοπάθεια και η μεταβατικότητα τής " | " έπεται από το (v) τής προτάσεως Β.1.3 και το (v) τής προτάσεως Β.1.5. Επιπροσθέτως, για κάθε ζεύγος $(a,b) \in \mathfrak{X} \times \mathfrak{X}$ με $a \mid b$ και $b \mid a$, ισχύει $a = |a| = |b| = b$ (λόγω τού (iii) τής προτάσεως Β.1.5). Άρα η " | " είναι *και* αντισυμμετρική επί τού $\mathfrak{X}$. Ωστόσο, το $(\mathfrak{X}, |)$ δεν είναι ολικώς διατεταγμένο σύνολο, διότι π.χ. $2 \nmid 3$. □

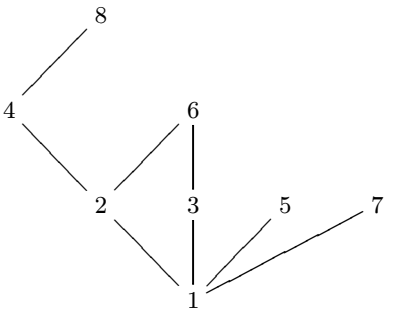
Β.2.31 Παρατήρηση. Προσοχή! Το ζεύγος $(\mathbb{Z}, |)$ δεν είναι μερικώς διατεταγμένο σύνολο, καθότι η " | " δεν είναι αντισυμμετρική επί τού $\mathbb{Z}$. Π.χ., $2 \mid -2$ και $-2 \mid 2$, αλλά $2 \neq -2$.

Β.2.32 Παράδειγμα. Θεωρούμε τα μερικώς διατεταγμένα σύνολα $(\mathbb{N}, |)$ και $(\mathbb{N}, \leq)$ (βλ. Β.2.30 και Α.2.2 (iii)). Η ταυτοτική απεικόνιση id: $(\mathbb{N}, |) \longrightarrow (\mathbb{N}, \leq)$ είναι αμφιριπτική και ισότονη από το ένα επί τού άλλου (διότι για $k, n \in \mathbb{N}$ ισχύει η συνεπαγωγή $k \mid n \Rightarrow k \leq n$) αλλά *δεν είναι* ισομορφισμός μερικώς διατεταγμένων συνόλων (υπό την έννοια τού ορισμού Α.2.9), διότι π.χ. $2 \leq 3$ και $2 \nmid 3$.

[7] Εάν $(a,b) \in \mathfrak{X} \times \mathfrak{X}$ και εάν $\exists c \in \mathbb{Z} : b = ac$, τότε κατ' ανάγκην $c \in \mathfrak{X}$. Κατά συνέπειαν, $[a \mid b \Leftrightarrow \exists c \in \mathfrak{X} : b = ac]$ για κάθε ζεύγος $(a,b) \in \mathfrak{X} \times \mathfrak{X}$.

Β.2.33 Σημείωση. Πολλά χρήσιμα (αριθμοθεωρητικά) παραδείγματα μερικώς διατεταγμένων συνόλων παρέχονται από *πεπερασμένα* υποσύνολα τού $\mathbb{N}$ (εφοδιαζόμενα με τη μερική διάταξη διαιρετότητας την επαγομένη επ' αυτών, βλ. εδάφιο Α.2.6). Ενδεικτικώς αναφέρονται τα ακόλουθα:

(i) Θεωρούμε το $(\mathfrak{X}, |)$, όπου $\mathfrak{X} := \{1, 2, 3, 4, 5, 6, 7, 8\}$. Οι αριθμοί $5, 6, 7$ και 8 είναι τα μεγιστικά στοιχεία τού $\mathfrak{X}$, ενώ το 1 είναι το ελάχιστο στοιχείο του (ως προς την " | "). Το $\mathfrak{X}$ *δεν διαθέτει* μέγιστο στοιχείο. Το αντίστοιχο διάγραμμα τού Hasse για το $(\mathfrak{X}, |)$ είναι το



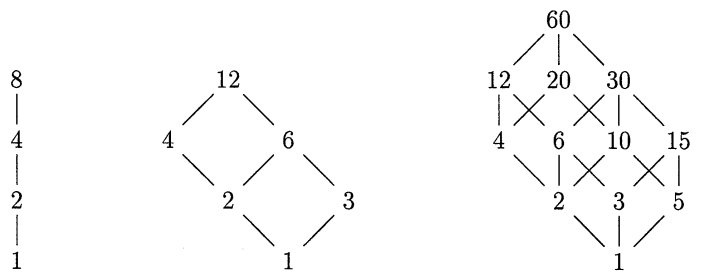
(ii) Θεωρούμε το μερικώς διατεταγμένο σύνολο $(\mathfrak{X}, |)$, όπου $\mathfrak{X} = \{3, 5, 30, 45\}$, καθώς και το $\mathfrak{Y} := \{3, 5\}$. Εν προκειμένω, $\mathrm{A}\Phi(\mathfrak{Y}; \mathfrak{X}) = \{30, 45\}$, αλλά το $\mathfrak{Y}$ δεν διαθέτει ελάχιστο άνω φράγμα εντός τού $\mathfrak{X}$ ως προς την "|".

Β.2.34 Παράδειγμα. Έστω $m \in \mathbb{N}$. Το σύνολο

$$\boxed{\mathfrak{D}_m := \{d \in \mathbb{N} : d \mid m\}}$$

όλων των θετικών ακεραίων διαιρετών τού m καθίσταται μερικώς διατεταγμένο μέσω τής σχέσεως διαιρετότητας " | " την επαγομένη από το $(\mathbb{N}, |)$ (βλ. Β.2.30 και Α.2.6).

(i) Τα διαγράμματα τού Hasse για τα $(\mathfrak{D}_8, |)$, $(\mathfrak{D}_{12}, |)$ και $(\mathfrak{D}_{60}, |)$, αντιστοίχως, είναι τα ακόλουθα:



(ii) Τα μερικώς διατεταγμένα σύνολα $(\mathfrak{D}_{30}, |)$ και $(\mathfrak{P}(\Omega), \subseteq)$, όπου $\Omega := \{\spadesuit, \clubsuit, \heartsuit\}$ (όπως στο Α.2.5), είναι ισόμορφα, καθότι η αμφίρριψη

$$1 \longmapsto \varnothing,\ 2 \longmapsto \{\spadesuit\},\ 3 \longmapsto \{\heartsuit\},\ 5 \longmapsto \{\clubsuit\},$$

$$6 \longmapsto \{\spadesuit, \heartsuit\},\ 10 \longmapsto \{\spadesuit, \clubsuit\},\ 15 \longmapsto \{\clubsuit, \heartsuit\},\ 30 \longmapsto \Omega$$

είναι ισότονη και έχει ισότονη αντίστροφο.

Β.2.35 Πρόταση. *Το μερικώς διατεταγμένο σύνολο* $(\mathfrak{X}, |)$, *όπου* $\mathfrak{X} \in \{\mathbb{N}, \mathbb{N}_0\}$, *αποτελεί έναν σύνδεσμο με*[8] $m \wedge n = \text{μκδ}(m,n),\ m \vee n = \text{εκπ}(m,n),\ \forall (m,n) \in \mathfrak{X} \times \mathfrak{X}$.

ΑΠΟΔΕΙΞΗ. Επειδή $\text{μκδ}(m,n) \mid m$ και $\text{μκδ}(m,n) \mid n$, για κάθε $(m,n) \in \mathfrak{X} \times \mathfrak{X}$, ο μέγιστος κοινός διαιρέτης $\text{μκδ}(m,n)$ των m και n αποτελεί κάτω φράγμα τού $\{m,n\}$ εντός τού $\mathfrak{X}$ ως προς την "|", και μάλιστα το *μέγιστο κάτω φράγμα*, διότι για οιονδήποτε $\delta \in \mathfrak{X}$, για τον οποίο ισχύει $\delta \mid m$ και $\delta \mid n$, έχουμε $\delta \mid \text{μκδ}(m,n)$. (Τούτο έπεται από το (iii) τής προτάσεως Β.1.3 όταν $\mathfrak{X} = \mathbb{N}_0$ και $\delta = 0$, και από το πόρισμα Β.2.6 όταν $\delta > 0$.) Κατ' αναλογίαν, επειδή $m \mid \text{εκπ}(m,n)$ και $n \mid \text{εκπ}(m,n)$, για κάθε $(m,n) \in \mathfrak{X} \times \mathfrak{X}$, το ελάχιστο κοινό πολλαπλάσιο $\text{εκπ}(m,n)$ των m και n αποτελεί άνω φράγμα τού $\{m,n\}$ εντός τού $\mathfrak{X}$ ως προς την "|", και μάλιστα *ελάχιστο άνω φράγμα*, διότι για οιονδήποτε $l \in \mathfrak{X}$, για τον οποίο ισχύει $m \mid l$ και $n \mid l$, έχουμε $\text{εκπ}(m,n) \mid l$. (Τούτο έπεται από το (i) τής προτάσεως Β.1.3 όταν $\mathfrak{X} = \mathbb{N}_0$ και $mn = 0$, και από την πρόταση Β.2.25 όταν $mn \neq 0$.)

Β.2.36 Πόρισμα. *Έστω* $m \in \mathbb{N}$. *Το μερικώς διατεταγμένο σύνολο* $(\mathfrak{D}_m, |)$ (το ορισθέν στο εδάφιο Β.2.34) *είναι ένας υποσύνδεσμος τού* $(\mathbb{N}, |)$, *διότι*

$$\text{μκδ}(k,l) \in \mathfrak{D}_m, \quad \text{εκπ}(k,l) \in \mathfrak{D}_m, \ \ \forall (k,l) \in \mathfrak{D}_m \times \mathfrak{D}_m.$$

ΑΠΟΔΕΙΞΗ. Εάν $(k,l) \in \mathfrak{D}_m \times \mathfrak{D}_m$, τότε $[\text{μκδ}(k,l) \mid k \text{ και } k \mid m] \underset{\text{Β.1.5 (v)}}{\Longrightarrow} \text{μκδ}(k,l) \mid m$ και $\text{εκπ}(k,l) \mid m$ (βλ. πόρισμα Β.3.21). □

Β.2.37 Πρόταση. *Εάν* $m_1, ..., m_r \in \mathbb{N}$ $(r \in \mathbb{N})$, *τότε*

$$\mathfrak{D}_{\text{μκδ}(m_1,\ldots,m_r)} = \mathfrak{D}_{m_1} \cap \cdots \cap \mathfrak{D}_{m_r}.$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το πόρισμα Β.2.6. □

Β.3 ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

Β.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 $n = n_1 n_2$.

Β.3.2 Πρόταση. *Κάθε* $n \in \mathbb{N}$, $n \geq 2$, *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 $2 \leq k_1 \leq k_2 < k$ 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 είναι πρώτος αριθμός. □

[8] Σημειωτέον ότι για $\mathfrak{X} = \mathbb{N}_0$ έχουμε $m \wedge 0 = 0 \wedge m = m$ και $m \vee 0 = 0 \vee m = 0$, για κάθε $m \in \mathbb{N}_0$.

Β.3.3 Θεώρημα. *Το σύνολο των πρώτων αριθμών είναι ένα απειροσύνολο*[9].

ΑΠΟΔΕΙΞΗ[10]. Ας υποθέσουμε ότι το σύνολο των πρώτων αριθμών είναι πεπερασμένο, ας πούμε το $\{p_1, p_2, ..., p_k\}$, κι ας θεωρήσουμε τον $m := p_1 p_2 \cdots p_k + 1$. Τότε ισχύει $p_1 \nmid m,\ p_2 \nmid m, ...,\ p_k \nmid m$ (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 αντέφασκε προς την ανισότητα $p_j > 1$). Τούτο όμως είναι άτοπο λόγω τής Β.3.2. □

Β.3.4 Θεώρημα. *Κάθε $n \in \mathbb{N}$, $n \geq 2$, γράφεται ως γινόμενο πρώτων αριθμών.*

ΑΠΟΔΕΙΞΗ[11]. Θα γίνει χρήση τής δεύτερης μορφής τής μαθηματικής επαγωγής. Για $n = 2$ το θεώρημα είναι αληθές. Υποθέτουμε ότι αυτό συμβαίνει και για τους $2, 3, ..., n-1$ και θεωρούμε τον 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. Άρα *και* σε αυτήν την περίπτωση ο n γράφεται ως γινόμενο πρώτων. □

Στην επόμενη ενότητα (και συγκεκριμένα στο θεώρημα Β.4.52) θα δοθεί μια ικανή και αναγκαία συνθήκη, ούτως ώστε ένας ακέραιος > 1 να είναι *πρώτος*.

Β.3.5 Λήμμα. *Εάν $m, n \in \mathbb{Z} \setminus \{0, \pm 1\}$ και p είναι ένας πρώτος αριθμός 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 Β.2.9. □

Β.3.6 Λήμμα. *Εάν $k \in \mathbb{N}$ και οι $p, p_1, ..., p_k$ είναι πρώτοι αριθμοί, τέτοιοι ώστε να ισχύει $p \mid p_1 \cdots p_k$, 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. Β.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, συνάγεται ότι $p = p_j$. □

Β.3.7 Θεώρημα. (Θεμελιώδες Θεώρημα τής Αριθμητικής) *Κάθε $n \in \mathbb{N}$, $n \geq 2$, γράφεται* μονοσημάντως *ως γινόμενο πρώτων αριθμών (μη λαμβανομένης υπ' όψιν τής διατάξεως των εμφανιζομένων παραγόντων εντός αυτού).*

ΑΠΟΔΕΙΞΗ. Κάτα το θεώρημα Β.3.4 κάθε $n \in \mathbb{N}$, $n \geq 2$, μπορεί να παρασταθεί ως γινόμενο πρώτων αριθμών. Αρκεί λοιπόν να αποδειχθεί το *μονοσήμαντο* τής

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

[10] 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.)

[11] 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.)

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

$$n = p_1 \cdots p_k = q_1 \cdots q_l, \tag{Β.18}$$

όπου $k, l \in \mathbb{N}$ και $p_1,...,p_k, q_1,...,q_l$ πρώτοι αριθμοί. Επιπροσθέτως, δίχως βλάβη τής γενικότητας, υποθέτουμε ότι $p_1 \le \cdots \le p_k$ και $q_1 \le \cdots \le q_l$. Χρησιμοποιώντας τή δεύτερη μορφή τής μαθηματικής επαγωγής ως προς τον n θα δείξουμε ότι $k = l$ και $p_j = q_j$ για κάθε $j \in \{1,...,k\}$. Για $n = 2$ το θεώρημα είναι αληθές. Υποθέτουμε ότι αυτό είναι αληθές και για κάθε φυσικό t, με $2 \le t < n$, όπου n οιοσδήποτε παγιωμένος φυσικός ≥ 3. Εάν ο n είναι πρώτος, τότε ο ισχυρισμός είναι αληθής. Εάν ο n είναι σύνθετος, τότε στην (Β.18) έχουμε $k \ge 2$ και $l \ge 2$. Επειδή ισχύει $p_1 \mid q_1 \cdots q_l$ και $q_1 \mid p_1 \cdots p_k$, υπάρχουν κάποιοι $j \in \{1,...,k\}$, $\varrho \in \{1,...,l\}$ με $q_1 = p_j$ και $p_1 = q_\varrho$ (κατά το λήμμα Β.3.6). Εξ αυτού έπεται ότι

$$[p_1 \le p_j = q_1 \text{ και } q_1 \le q_\varrho = p_1] \Longrightarrow p_1 = q_1,$$

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 έχουμε $k - 1 = l - 1$ και $p_j = q_j$, για κάθε $j \in \{2,...,k\}$. Ως εκ τούτου, $k = l$ και $p_j = q_j$, για κάθε $j \in \{1,...,k\}$. □

Β.3.8 Ορισμός. Από το θεώρημα Β.3.7 έπεται ότι κάθε φυσικός αριθμός $n \ge 2$ μπορεί να γραφεί *μονοσημάντως* ως

$$\boxed{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},} \tag{Β.19}$$

όπου $k \in \mathbb{N}$, οι $p_1, p_2,..., p_k$ είναι σαφώς διακεκριμένοι πρώτοι αριθμοί με

$$p_1 < p_2 < \cdots < p_k$$

(όταν $k \ge 2$) και οι $\alpha_1, \alpha_2,..., \alpha_k$ φυσικοί αριθμοί. Η έκφραση (Β.19) καλείται **κανονική παράσταση τού n ως γινομένου πρώτων αριθμών** ή **κανονική αποσύνθεση τού n σε γινόμενο πρώτων αριθμών** (ή **πρώτων παραγόντων**).

Β.3.9 Παράδειγμα. Το 1, καθώς και οι κανονικές παραστάσεις (Β.19) όλων των φυσικών αριθμών n, όπου $2 \le n \le 100$, περιλαμβάνονται στον κατάλογο

n	Παρ.	n	Παρ.	n	Παρ.	n	Παρ.	n	Παρ.
1	1	11	11	21	$3 \cdot 7$	31	31	41	41
2	2	12	$2^2 \cdot 3$	22	$2 \cdot 11$	32	2^5	42	$2 \cdot 3 \cdot 7$
3	3	13	13	23	23	33	$3 \cdot 11$	43	43
4	2^2	14	$2 \cdot 7$	24	$2^3 \cdot 3$	34	$2 \cdot 17$	44	$2^2 \cdot 11$
5	5	15	$3 \cdot 5$	25	5^2	35	$5 \cdot 7$	45	$3^2 \cdot 5$
6	$2 \cdot 3$	16	2^4	26	$2 \cdot 13$	36	$2^2 \cdot 3^2$	46	$2 \cdot 23$
7	7	17	17	27	3^3	37	37	47	47
8	2^3	18	$2 \cdot 3^2$	28	$2^2 \cdot 7$	38	$2 \cdot 19$	48	$2^4 \cdot 3$
9	3^2	19	19	29	29	39	$3 \cdot 13$	49	7^2
10	$2 \cdot 5$	20	$2^2 \cdot 5$	30	$2 \cdot 3 \cdot 5$	40	$2^3 \cdot 5$	50	$2 \cdot 5^2$

όταν $n \leq 50$ και στον κατάλογο

n	Παρ.	n	Παρ.	n	Παρ.	n	Παρ.	n	Παρ.
51	$3 \cdot 17$	61	61	71	71	81	3^4	91	$7 \cdot 13$
52	$2^2 \cdot 13$	62	$2 \cdot 31$	72	$2^3 \cdot 3^2$	82	$2 \cdot 41$	92	$2^2 \cdot 23$
53	53	63	$3^2 \cdot 7$	73	73	83	83	93	$3 \cdot 31$
54	$2 \cdot 3^3$	64	2^6	74	$2 \cdot 37$	84	$2^2 \cdot 3 \cdot 7$	94	$2 \cdot 47$
55	$5 \cdot 11$	65	$5 \cdot 13$	75	$3 \cdot 5^2$	85	$5 \cdot 17$	95	$5 \cdot 19$
56	$2^3 \cdot 7$	66	$2 \cdot 3 \cdot 11$	76	$2^2 \cdot 19$	86	$2 \cdot 43$	96	$2^5 \cdot 3$
57	$3 \cdot 19$	67	67	77	$7 \cdot 11$	87	$3 \cdot 29$	97	97
58	$2 \cdot 29$	68	$2^2 \cdot 17$	78	$2 \cdot 3 \cdot 13$	88	$2^3 \cdot 11$	98	$2 \cdot 7^2$
59	59	69	$3 \cdot 23$	79	79	89	89	99	$3^2 \cdot 11$
60	$2^2 \cdot 3 \cdot 5$	70	$2 \cdot 5 \cdot 7$	80	$2^4 \cdot 5$	90	$2 \cdot 3^2 \cdot 5$	100	$2^2 \cdot 5^2$

όταν $51 \leq n \leq 100$.

Β.3.10 Παρατήρηση. Προφανώς, κάθε *ακέραιος* $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ μπορεί να γραφεί *μονοσημάντως* ως

$$n = \text{sign}\,(n)\ p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{Β.20}$$

όπου $k \in \mathbb{N}$, οι $p_1, p_2, ..., p_k$ πρώτοι αριθμοί με $p_1 < \cdots < p_k$ και οι $\alpha_1, ..., \alpha_k$ φυσικοί αριθμοί. Αλλά ακόμη και κάθε $n \in \mathbb{Q} \setminus \{0, \pm 1\}$ μπορεί να παρασταθεί *μονοσημάντως* υπό τη μορφή (Β.20), όπου -εν προκειμένω- $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{Z} \setminus \{0\}$. Από το θεώρημα Β.3.7 και τις (Β.19), (Β.20) έχει γίνει πλέον αντιληπτό το γιατί οι πρώτοι αριθμοί θεωρούνται *δομικοί λίθοι* μέσω των οποίων «κτίζονται» τα σύνολα $\mathbb{N}, \mathbb{Z}$ και $\mathbb{Q}$. Εντούτοις, η κατανομή τους εντός τού $\mathbb{N}$ είναι αξιοπερίεργη, ελέγχεται δε (όπως δείχνει το λεγόμενο *θεώρημα των πρώτων αριθμών*) μόνον ασυμπτωτικώς.

Β.3.11 Θεώρημα. («Θεώρημα των πρώτων αριθμών») *Το πλήθος των πρώτων αριθμών που είναι μικρότεροι ή ίσοι ενός θετικού πραγματικού αριθμού x πλησιάζει ασυμπτωτικώς τον λόγο $x/\ln(x)$ (τού x τείνοντος στο ∞), ήτοι*

$$\lim_{x \to \infty} \left(\frac{\text{card}(\{\, p \text{ πρώτος} | \, p \leq x\})}{x/\ln(x)} \right) = 1.$$

Οι πρώτες δύο (αναλυτικές) αποδείξεις[12] τού θεωρήματος Β.3.11 (βασιζόμενες σε ιδιότητες τής συναρτήσεως ζήτα τού Riemann) εδόθησαν από τους Charles Jean de

[12] Για «στοιχειωδέστερες» (αλλά μακροσκελείς) αποδείξεις βλ.

P. Erdös: *A new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 374-384, και

A. Selberg: *An elementary proof of the prime number theory*, Annals of Math. **50** (1949), 305-313.

► Για την ιστορική διαδρομή αυτού τού θεωρήματος, βλ.

L.J. Goldstein: *A History of the Prime Number Theorem*, American Math. Monthly **80** (1973), 599-741, και

P.T. Bateman & H.G. Diamond: *A hundred years of prime numbers*, American Math. Monthly **103** (1996), 729-741.

► Για μια λεπτομερή απόδειξή του (στο πλαίσιο τής Αναλυτικής Θεωρίας Αριθμών) βλ.

G.J.O. Jameson: *The Prime Number Theorem*, London Math. Soc. Student Texts, Vol. **53**, Cambridge Un. Press, 2003.

la Vallée-Poussin (1866-1962) και Jacques Hadamard (1865-1963) και δημοσιεύθηκαν το έτος 1896. Σημειωτέον ότι εντός τού $\mathbb{N}$ υφίστανται *μεγάλα* διαστήματα στα οποία δεν συναντούμε πρώτους αριθμούς[13]. Η ύπαρξη *αυθαιρέτως μεγάλων* «χασμάτων» μεταξύ *κάποιων* διαδοχικών πρώτων αριθμών προκύπτει από την ακόλουθη:

Β.3.12 Πρόταση. *Δοθέντος ενός $n \in \mathbb{N}$, $n \geq 2$, υπάρχουν πάντοτε n διαδοχικοί σύνθετοι αριθμοί.*

ΑΠΟΔΕΙΞΗ. Οι n διαδοχικοί φυσικοί αριθμοί

$$m_k := (n+1)! + k,\ k \in \{2, 3, ..., n+1\},$$

είναι σύνθετοι, διότι $k \mid (n+1)! \Rightarrow k \mid m_k$ για κάθε $k \in \{2, 3, ..., n+1\}$. □

Στο άλλο άκρο, τώρα, υπάρχουν στοιχειωδώς περιγραφόμενα *ευδιάκριτα* γνήσια υποσύνολα τού $\mathbb{N}$ τα οποία περιέχουν *άπειρους* πρώτους αριθμούς. Είναι, μάλιστα, εντυπωσιακό το ότι μεταξύ αυτών συγκαταλέγονται και τα σύνολα των όρων *κατάλληλων αριθμητικών προόδων*.

Β.3.13 Θεώρημα. (G.L. Dirichlet, 1837.) *Εάν $a, b \in \mathbb{N}$ με* μκδ$(a, b) = 1$, *τότε εντός τού συνόλου $\{a + nb | n \in \mathbb{N}\}$ υπάρχουν άπειροι πρώτοι αριθμοί.*

Ο G.L. Dirichlet[14] (1805-1859) απέδειξε το θεώρημα Β.3.13 με αναλυτικά μέσα, κάνοντας χρήση των λεγομένων *L-σειρών*. Διαφορετικές αποδείξεις οφείλονται στους H. Zassenhaus[15], A. Selberg[16], H.N. Shapiro[17] κ.ά. Για την ειδική περίπτωση όπου $a = 1$, υπάρχουν και στοιχειωδέστερες αποδείξεις. (Κατ' ουσίαν, αρκούν κατάλληλοι χειρισμοί των ιδιοτήτων είτε τού *κυκλοτομικού πολυωνύμου*[18] είτε τής *συναρτήσεως* Β.4.32 *τού Möbius*[19].)

[13] Επί παραδείγματι, ο πρώτος αριθμός 370261 ακολουθείται από 111 σύνθετους αριθμούς και καθένας εκ των 209 φυσικών αριθμών που βρίσκονται μεταξύ των 20831323 και 20831533 είναι σύνθετος.

[14] G.L. Dirichlet: *Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin (1837), 45-81. Για πιο σύγχρονες παρουσιάσεις βλ.

E. Landau: *Elementary Number Theory*, translated by J.E. Goodman, Chealsea Pub. Co., 1958, Ch. III, σελ. 104-125,

H. Hasse: *Vorlesungen über Zahlentheorie*, zweite Aufl., Springer-Verlag, 1964, σελ. 176-283,

Z.I. Borevich & I.R. Shafarevich: *Number Theory*, transl. by N. Greenleaf, Academic Press, 1966, σελ. 339-341,

J.-P. Serre: *A Course in Arithmetic*, GTM, Vol. **7**, Springer-Verlag, 1973, Ch. VI, σελ. 61-76, και

T. Apostol: *Εισαγωγή στην Αναλυτική Θεωρία των Αριθμών*, σε μετ. των Α. και Ε. Ζαχαρίου, και επιμ. Γ. Λεγάτου, εκδόσεις Gutenberg, Αθήνα 1986, Κεφ. 7, σελ. 198-208.

[15] H. Zassenhaus: *Über die Existenz von Primzahlen in arithmetischen Progressionen*, Commentarii Mathematici Helvetici **22** (1949), 232-259.

[16] A.Selberg: *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Annals of Mathematics **50** (1949), 297-304.

[17] H.N. Shapiro: *On primes in arithmetic progressions I, II*, Annals of Mathematics **52** (1950), 217-243.

[18] Βλ. P. Ribenboim: *The New Book of Prime Number Records*, Springer-Verlag, 1996, σελ. 268.

[19] Βλ. H. Gauchman: *A special case of Dirichlet's theorem on primes in an arithmetic progression*, Mathematics Magazine **74** (2001), 397-399.

Β.3.14 Λήμμα. *Έστω n ένας φυσικός αριθμός γραφόμενος υπό τη μορφή*

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

όπου $k \in \mathbb{N}$, οι $p_1, p_2, ..., p_k$ πρώτοι αριθμοί σαφώς διακεκριμένοι (για $k > 1$) και οι $\alpha_1, \alpha_2, ..., \alpha_k$ μη αρνητικοί ακέραιοι αριθμοί. Τότε ένας φυσικός αριθμός m διαιρεί τον n εάν και μόνον εάν

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

όπου $\beta_1, \beta_2, ..., \beta_k \in \mathbb{N}_0$ με $0 \leq \beta_j \leq \alpha_j$, για κάθε $j \in \{1, ..., k\}$.

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

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

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

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

τότε υπάρχει $r \in \mathbb{N}$, τέτοιος ώστε να ισχύει η ισότητα

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

Από τη μοναδικότητα τής παραστάσεως τού n ως γινομένου πρώτων παραγόντων λαμβάνουμε $l \leq k$ και $q_\varrho = p_{j_\varrho}$, $0 < \gamma_\varrho \leq \alpha_{j_\varrho}$, $\forall \varrho \in \{1, ..., l\}$, για κάποιο υποσύνολο δεικτών $\{j_1, ..., j_\varrho\} \subseteq \{1, ..., k\}$. Ως εκ τούτου, οιοσδήποτε φυσικός αριθμός $m \geq 1$ διαιρεί τον n θα γράφεται υπό την επιθυμητή μορφή. □

Β.3.15 Πρόταση. *Έστω $n \in \mathbb{N}$. Εάν $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, όπου $k \in \mathbb{N}$, $p_1, p_2, ..., p_k$ πρώτοι αριθμοί σαφώς διακεκριμένοι (για $k > 1$) και $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}_0$, τότε ισχύουν τα ακόλουθα*:

(i) *Για τον πληθικό αριθμό τού συνόλου $\mathfrak{D}_n$ των θετικών ακεραίων διαιρετών τού n* (βλ. Β.2.34) *έχουμε*

$$\boxed{\text{card}(\mathfrak{D}_n) = \prod_{j=1}^{k} (\alpha_j + 1).}$$

(ii) *Το άθροισμα των θετικών ακεραίων διαιρετών τού n δίδεται από τον τύπο*

$$\boxed{\sum_{d \in \mathfrak{D}_n} d = \prod_{j=1}^{k} \left(\frac{p_j^{\alpha_j + 1} - 1}{p_j - 1} \right).} \tag{B.21}$$

ΑΠΟΔΕΙΞΗ. (i) Κατά το λήμμα Β.3.14 οι θετικοί ακέραιοι διαιρέτες τού n είναι τής μορφής

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \ \text{όπου} \ 0 \le \beta_j \le \alpha_j, \ \forall j \in \{1, ..., k\}.$$

Επομένως υπάρχουν ακριβώς $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ θετικοί διαιρέτες τού n.

(ii) Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον k. Εάν $k = 1$, τότε (κατά το λήμμα Β.3.14) οι θετικοί ακέραιοι διαιρέτες τού n είναι οι $1, p_1, p_1^2, ..., p_1^{\alpha_1}$ και το άθροισμά τους ισούται με

$$1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1} = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}.$$

Εάν $k > 1$, θέτουμε $l := p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}$. Σύμφωνα με την επαγωγική μας υπόθεση,

$$\sum_{d \in \mathfrak{D}_l} d = \prod_{j=1}^{k-1} \left(\frac{p_j^{\alpha_j+1} - 1}{p_j - 1} \right). \tag{Β.22}$$

Επειδή $\mathfrak{D}_n = \left\{ c p_k^{\beta_k} \,\middle|\, c \in \mathfrak{D}_l, \beta_k \in \{0, 1, ..., \alpha_k\} \right\}$, έχουμε

$$\sum_{d \in \mathfrak{D}_n} d = \sum_{d \in \mathfrak{D}_l} d + \left(\sum_{d \in \mathfrak{D}_l} d \right) p_k + \left(\sum_{d \in \mathfrak{D}_l} d \right) p_k^2 + \cdots + \left(\sum_{d \in \mathfrak{D}_l} d \right) p_k^{\alpha_k},$$

οπότε

$$\sum_{d \in \mathfrak{D}_n} d = \left(\sum_{d \in \mathfrak{D}_l} d \right) \left(1 + p_k + p_k^2 + \cdots + p_k^{\alpha_j} \right) = \left(\sum_{d \in \mathfrak{D}_l} d \right) \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \tag{Β.23}$$

Η (Β.21) προκύπτει άμεσα από τις (Β.22) και (Β.23). □

Β.3.16 Πρόταση. *Εάν $n \in \mathbb{N}, \ n \ge 2$, και $a_1, ..., a_n \in \mathbb{Z} \setminus \{0\}$ με*

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

όπου $p_1, ..., p_k$ είναι πρώτοι αριθμοί σαφώς διακεκριμένοι (όταν $k > 1$) και οι $\alpha_{j,l}$, $j \in \{1, ..., n\}, \ l \in \{1, ..., k\}$, μη αρνητικοί ακέραιοι αριθμοί, τότε

$$\boxed{\text{μκδ}(a_1, ..., a_n) = \prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l}, ..., \alpha_{n,l}\}}.} \tag{Β.24}$$

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

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

έχουμε $\prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l},...,\alpha_{n,l}\}} \mid a_j$, για κάθε $j \in \{1,...,n\}$ (βλ. Β.3.14). Επιπροσθέτως, εάν δ είναι οιοσδήποτε φυσικός αριθμός, για τον οποίο ισχύει $\delta \mid a_1$,..., $\delta \mid a_n$, τότε, κατά το λήμμα Β.3.14, $\delta = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$, όπου

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

οπότε $\delta_l \leq \min\{\alpha_{1,l},...,\alpha_{n,l}\}$, $\forall l \in \{1,...,k\} \Rightarrow \delta \mid \prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l},...,\alpha_{n,l}\}}$. Επομένως η (Β.24) είναι αληθής λόγω τού πορίσματος Β.2.6. □

Β.3.17 Πόρισμα. *Εάν $n \in \mathbb{N},\ n \geq 2$, και $a, b_1,...,b_n \in \mathbb{Z} \setminus \{0\}$ με τους $b_1,...,b_n$ ανά δύο σχετικώς πρώτους, τότε*

$$\text{μκδ}(a, \prod_{j=1}^{n} b_j) = \prod_{j=1}^{n} \text{μκδ}(a, b_j). \tag{Β.25}$$

ΑΠΟΔΕΙΞΗ. Αρκεί να αποδείξουμε την ισότητα (Β.25) στην περίπτωση κατά την οποία οι ως άνω αριθμοί είναι φυσικοί ≥ 2. Εφαρμόζουμε την πρώτη μορφή τής μαθηματικής επαγωγής ως προς τον n 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 $b_1 = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $b_2 = q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_l^{\gamma_l}$, τότε οι $p_1, p_2,..., p_k, q_1, q_2,..., q_l$ είναι σαφώς διακεκριμένοι πρώτοι αριθμοί, καθόσον $\text{μκδ}(b_1, b_2) = 1$. Γράφοντας τον a ως γινόμενο σαφώς 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,δ_2,..., $\delta_k, \varepsilon_1, \varepsilon_2,..., \varepsilon_l \in \mathbb{N}_0$ κατάλληλοι εκθέτες των πρώτων που εμφανίζονται στις αποσυνθέσεις των b_1, b_2 και $r_1, r_2,..., r_m$ οι πρώτοι που εμφανίζονται στην αποσύνθεση τού a, αλλά δεν περιέχονται στις αποσυνθέσεις των b_1, b_2, υψωμένοι σε κατάλληλες δυνάμεις $\zeta_1, \zeta_2,..., \zeta_m \in \mathbb{N}$. Εφαρμόζοντας την (Β.24) 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 (Β.25) είναι αληθής για κάποιον $n = k \geq 2$, θα την αποδείξουμε και για $n = k + 1$. Παρατηρούμε ότι $\text{μκδ}(b_1 b_2 \cdots b_k, b_{k+1}) = 1$ (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 $j \in \{1,...,k\}$ 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 (Β.25) είναι αληθής και για $n = k + 1$. □

Β.3.18 Πόρισμα. *Εστω ότι* $n \in \mathbb{N},\ n \geq 2$, *και ότι* $a, b_1,...,b_n \in \mathbb{Z}\setminus\{0\}$ *με τους* $b_1,...,b_n$ *ανά δύο σχετικώς πρώτους. Εάν* $b_j \mid a, \forall j \in \{1,...,n\}$, *τότε* $\prod_{j=1}^{n} b_j \mid a$.

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το πόρισμα Β.3.17 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 $\prod_{j=1}^{n} b_j \mid a$. □

Β.3.19 Πόρισμα. *Εάν* $n \in \mathbb{N},\ n \geq 2$, *και οι* $a_1,...,a_n$ *είναι μη μηδενικοί ακέραιοι, ανά δύο σχετικώς πρώτοι, τότε* $\text{εκπ}(a_1,...,a_n) = |a_1 \cdots a_n|$.

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

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

(βλ. Β.2.25 (ii)). Εξάλλου επειδή εξ ορισμού $a_j \mid \text{εκπ}(a_1,...,a_n)$ για κάθε δείκτη $j \in \{1,...,n\}$ και οι $a_1,...,a_n$ είναι σχετικώς πρώτοι ανά δύο,

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

(βλ. Β.3.18 και Β.1.5 (i)). Επειδή τόσο το $\text{εκπ}(a_1,...,a_n)$ όσο και ο $|a_1 \cdots a_n|$ είναι θετικοί ακέραιοι, από το (iii) τής προτάσεως Β.1.5 συμπεραίνουμε ότι οφείλουν να είναι ίσοι. □

Β.3.20 Πρόταση. *Εάν* $n \in \mathbb{N},\ n \geq 2$, *και* $a_1,...,a_n \in \mathbb{Z}\setminus\{0\}$ *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 $p_1,...,p_k$ *είναι πρώτοι αριθμοί σαφώς διακεκριμένοι* (*όταν* $k > 1$) *και οι* $\alpha_{j,l}$, $j \in \{1,...,n\},\ l \in \{1,...,k\}$, *μη αρνητικοί ακέραιοι αριθμοί, τότε*

$$\boxed{\text{εκπ}(a_1,...,a_n) = \prod_{l=1}^{k} p_l^{\max\{\alpha_{1,l},...,\alpha_{n,l}\}}.} \tag{Β.26}$$

ΑΠΟΔΕΙΞΗ. Επειδή $\text{εκπ}(a_1,...,a_n) = \text{εκπ}(|a_1|,...,|a_n|)$, μπορούμε -χωρίς βλάβη τής γενικότητας- να υποθέσουμε ότι οι $a_1,...,a_n$ 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 $a_j \mid \prod_{l=1}^{k} p_l^{\max\{\alpha_{1,l},...,\alpha_{n,l}\}}$, για κάθε $j \in \{1,...,n\}$ (βλ. Β.3.14). Επιπροσθέτως, εάν μ είναι οιοσδήποτε φυσικός αριθμός, για τον οποίο ισχύει $a_1 \mid \mu,...,\ a_n \mid \mu$, τότε, κατά το λήμμα Β.3.14,

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

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

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

οπότε $[\max\{\alpha_{1,l}, ..., \alpha_{n,l}\} \leq \mu_l, \ \forall l \in \{1, ..., k\}] \Longrightarrow \prod_{l=1}^{k} p_l^{\max\{\alpha_{1,l},...,\alpha_{n,l}\}} \mid \mu$. Επομένως η (B.26) είναι αληθής λόγω τής προτάσεως B.2.25. □

B.3.21 Πόρισμα. *Εάν* $m \in \mathbb{N}$, *τότε* $\text{εκπ}(k, l) \in \mathfrak{D}_m, \forall (k, l) \in \mathfrak{D}_m \times \mathfrak{D}_m$.

ΑΠΟΔΕΙΞΗ. Εάν $(k, l) \in \mathfrak{D}_m \times \mathfrak{D}_m$ και εάν (δίχως βλάβη τής γενικότητας) υποθέσουμε ότι

$$k = p_1^{\alpha_1} \cdots p_\nu^{\alpha_\nu}, \ l = p_1^{\beta_1} \cdots p_\nu^{\beta_\nu}, \ m = p_1^{\gamma_1} \cdots p_\nu^{\gamma_\nu}, \ (\nu \in \mathbb{N})$$

όπου οι $p_1,..., p_\nu$ είναι πρώτοι αριθμοί σαφώς διακεκριμένοι (για $\nu > 1$) και οι $\alpha_1,..., \alpha_\nu, \beta_1,..., \beta_\nu$ και $\gamma_1,..., \gamma_\nu$ μη αρνητικοί ακέραιοι αριθμοί, τότε

$$\left.\begin{array}{l} k \mid m \Rightarrow \alpha_j \leq \gamma_j, \ \forall j \in \{1, ..., \nu\} \\ l \mid m \Rightarrow \beta_j \leq \gamma_j, \ \forall j \in \{1, ..., \nu\} \end{array}\right\} \Rightarrow \max\{\alpha_j, \beta_j\} \leq \gamma_j, \ \forall j \in \{1, ..., \nu\},$$

οπότε $\text{εκπ}(k, l) \in \mathfrak{D}_m$ (μέσω τού λήμματος B.3.14 και τής προτάσεως B.3.20). □

B.3.22 Ορισμός. Έστω $x \in \mathbb{R}$. Ως **δάπεδο**[20] **(ή ακέραιο μέρος) τού** x ορίζεται ο ακέραιος αριθμός

$$\lfloor x \rfloor := \max\{ m \in \mathbb{Z} | \, m \leq x\}.$$

B.3.23 Σημείωση. Για οιουσδήποτε $x, y \in \mathbb{R}$ και $l \in \mathbb{Z}$ έχουμε

$$\lfloor x \rfloor \leq x \leq \lfloor x \rfloor + 1, \ \lfloor x + l \rfloor = \lfloor x \rfloor + l, \ \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor .$$

B.3.24 Πρόταση. (A.de Polignac & A.M. Legendre, 1808.) *Έστω* $n \in \mathbb{N}$, $n \geq 2$, *και έστω* p *ένας πρώτος αριθμός. Ο* p *εμφανίζεται στην κανονική παράσταση τού* ***παραγοντικού*** $n! := \prod_{i=1}^{n} i$ *τού* n *ως γινομένου πρώτων αριθμών υψωμένος στη δύναμη*

$$\boxed{\varepsilon_p(n) = \sum_{\nu=1}^{\lfloor \log_p(n) \rfloor} \left\lfloor \frac{n}{p^\nu} \right\rfloor .} \tag{B.27}$$

Ως εκ τούτου, εάν $\{p \in \mathbb{N} | \, p\text{πρώτος } \leq n\} = \{p_1, ..., p_k\}$ (όπου $p_1 < \cdots < p_k$ όταν $k \geq 2$), *τότε*

$$\boxed{n! = \prod_{j=1}^{k} p_j^{\varepsilon_{p_j}(n)}, \text{ όπου } \varepsilon_{p_j}(n) = \sum_{\nu=1}^{\lfloor \log_p(n) \rfloor} \left\lfloor \tfrac{n}{p_j^\nu} \right\rfloor, \ \forall j \in \{1, ..., k\}.}$$

[20] Κατ' αντιδιαστολήν προς την **οροφή** $\lceil x \rceil := \min\{ n \in \mathbb{Z} \mid \ n \geq x\}$ τού x που είναι ωσαύτως χρήσιμος αριθμός για ποικίλα προβλήματα τής Θεωρίας Αριθμών και τής Συνδυαστικής.

ΑΠΟΔΕΙΞΗ. Έστω $l \in \mathbb{N} : l \leq n$. Εάν $p^\nu \mid l$, για κάποιον $\nu \in \mathbb{N}$, τότε $p^\nu \leq l \leq n$, οπότε $\nu \leq \frac{\ln(n)}{\ln(p)} = \log_p(n)$. Επειδή $\nu \in \mathbb{N}$, έχουμε $\nu \leq \lfloor \log_p(n) \rfloor$. Κατά συνέπειαν, ο μέγιστος $\varepsilon_p(n) \in \mathbb{N}_0$, για τον οποίο ισχύει $p^{\varepsilon_p(n)} \mid n!$, είναι ο

$$\varepsilon_p(n) = \sum_{l=1}^{n} \sum_{\left\{\nu\in\mathbb{N}:1\leq\nu\leq\left\lfloor\log_p(n)\right\rfloor,\ \text{όπου } p^\nu\mid l\right\}} 1.$$

Επομένως,

$$\varepsilon_p(n) = \sum_{\nu=1}^{\lfloor\log_p(n)\rfloor} \sum_{\{l\in\mathbb{N}:1\leq l\leq n,\ \text{όπου } p^\nu\mid l\}} 1 = \sum_{\nu=1}^{\lfloor\log_p(n)\rfloor} \left\lfloor \frac{n}{p^\nu} \right\rfloor,$$

διότι για οιονδήποτε $\nu \in \left\{1, ..., \lfloor \log_p(n) \rfloor\right\}$, τα μόνα θετικά πολλαπλάσια l τού p^ν που είναι $\leq n$, είναι τα $p^\nu, 2p^\nu, ..., q_\nu p^\nu$, όπου

$$q_\nu := \max\{\, m \in \mathbb{N} |\, mp^\nu \leq n\} = \max\left\{ m \in \mathbb{Z} \,\middle|\, m \leq \frac{n}{p^\nu} \right\} =: \left\lfloor \frac{n}{p^\nu} \right\rfloor,$$

οπότε η (Β.27) είναι αληθής. □

Β.3.25 Παράδειγμα. Εάν $n = 10$, τότε οι πρώτοι αριθμοί που είναι ≤ 10 είναι οι $2, 3, 5$ και 7. Επειδή

$$\lfloor \log_2(10) \rfloor = \left\lfloor \tfrac{\ln 10}{\ln 2} \right\rfloor = \left\lfloor \tfrac{2{,}3025....}{0{,}69315...} \right\rfloor = \lfloor 3{,}321.... \rfloor = 3, \ \left\lfloor \tfrac{\ln 10}{\ln 3} \right\rfloor = 2$$

και $\left\lfloor \frac{\ln 10}{\ln 5} \right\rfloor = \left\lfloor \frac{\ln 10}{\ln 7} \right\rfloor = 1$, έχουμε

$$\varepsilon_2(10) = \left\lfloor \tfrac{10}{2} \right\rfloor + \left\lfloor \tfrac{10}{4} \right\rfloor + \left\lfloor \tfrac{10}{8} \right\rfloor = 5 + 2 + 1 = 8,$$
$$\varepsilon_3(10) = \left\lfloor \tfrac{10}{3} \right\rfloor + \left\lfloor \tfrac{10}{9} \right\rfloor = 4,\ \varepsilon_5(10) = \left\lfloor \tfrac{10}{5} \right\rfloor = 2,\ \varepsilon_7(10) = \left\lfloor \tfrac{10}{7} \right\rfloor = 1,$$

οπότε $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 = 3628\,800$.

Β.3.26 Πόρισμα. *Για κάθε πρώτον αριθμό p και για κάθε $s \in \mathbb{N}$ έχουμε*

$$\boxed{\varepsilon_p(p^s) = \tfrac{p^s - 1}{p - 1}.} \tag{Β.28}$$

ΑΠΟΔΕΙΞΗ. Προφανώς,

$$\varepsilon_p(p^s) = \sum_{\nu=1}^{s} \left\lfloor \frac{p^s}{p^\nu} \right\rfloor = p^{s-1} + p^{s-2} + \cdots + p + 1,$$

απ' όπου έπεται άμεσα η (Β.28). □

Β.3.27 Πόρισμα. *Έστω $n \in \mathbb{N}$, $n \geq 2$, και έστω p ένας πρώτος αριθμός. Εάν $r := \lfloor \log_p(n) \rfloor$ και*

$$n = c_r p^r + c_{r-1} p^{r-1} + \cdots + c_1 p + c_0$$

είναι η παράσταση (B.3) *τού* n *στην κλίμακα τού* p (*ήτοι στο "*p*-αδικό σύστημα"*), *τότε*

$$\boxed{\varepsilon_p(n) = \tfrac{n-(c_r+c_{r-1}+\cdots+c_1+c_0)}{p-1}.} \tag{B.29}$$

ΑΠΟΔΕΙΞΗ. Για $\nu \in \{1,...,r\}$ έχουμε

$$\tfrac{n}{p^\nu} = \tfrac{c_r p^r + c_{r-1}p^{r-1}+\cdots+c_1 p+c_0}{p^\nu} = c_r p^{r-\nu} + c_{r-1}p^{r-1-\nu} + \cdots + c_\nu + \tfrac{c_{\nu-1}p^{\nu-1}+\cdots+c_0}{p^\nu},$$

όπου $c_i \in \{0,1,...,p-1\}$ για κάθε $i \in \{0,...,r-1\}$ και $c_r \in \{1,...,p-1\}$. Επομένως,

$$\tfrac{c_{\nu-1}p^{\nu-1}+c_{\nu-2}p^{\nu-2}\cdots+c_0}{p^\nu} \le \tfrac{(p-1)(p^{\nu-1}+p^{\nu-2}+\cdots+1)}{p^\nu} = \tfrac{p^\nu-1}{p^\nu} < 1$$
$$\Longrightarrow \left\lfloor \tfrac{n}{p^\nu} \right\rfloor = c_\nu + \cdots + c_{r-1}p^{r-1-\nu} + c_r p^{r-\nu}$$

και η (B.27) δίδει

$$\begin{aligned}\varepsilon_p(n) = \sum_{\nu=1}^{r} \left\lfloor \frac{n}{p^\nu} \right\rfloor = c_1 + c_2 p + c_3 p^2 + \cdots + c_r p^{r-1} \\ +c_2 + c_3 p + \cdots + c_r p^{r-2} \\ +c_3 + \cdots + c_r p^{r-3} \\ \cdots\cdots \\ +c_r\end{aligned}$$

ήτοι

$$\begin{aligned}\varepsilon_p(n) &= c_1\tfrac{p-1}{p-1} + c_2\tfrac{p^2-1}{p-1} + c_3\tfrac{p^3-1}{p-1} + \cdots + c_r\tfrac{p^r-1}{p-1} \\ &= \tfrac{(c_r p^r + c_{r-1}p^{r-1}+\cdots+c_1 p+c_0)-(c_r+c_{r-1}+\cdots+c_1+c_0)}{p-1},\end{aligned}$$

οπότε η (B.29) είναι αληθής. □

B.3.28 Παράδειγμα. Επειδή για $n = 10$ έχουμε $10 = (1010)_2 = (101)_3 = (20)_5 = (13)_7$, οι υπολογισμοί τού εδ. B.3.25 μπορούν να εκτελεσθούν *και* μέσω τής (B.29) ως ακολούθως:

$$\varepsilon_2(10) = 10 - (1+0+1+0) = 8, \;\; \varepsilon_3(10) = \tfrac{10-(1+0+1)}{2} = 4,$$
$$\varepsilon_5(10) = \tfrac{10-(2+0)}{4} = 2, \;\; \varepsilon_7(10) = \tfrac{10-(1+3)}{6} = 1.$$

B.3.29 Παράδειγμα. Έστω $n \in \mathbb{N}$, $n \ge 2$. Από το πόρισμα B.3.27 έπεται ότι η μέγιστη δύναμη τού 2 που διαιρεί τον $n!$ είναι η 2^{n-k}, όπου ως k σημειώνουμε το πλήθος των μονάδων των εμφανιζομένων στο δυαδικό ανάπτυγμα τού n. Κατά συνέπειαν, $2^n \nmid n!$. Επιπλέον, $2^{n-1} \mid n!$ εάν και μόνον εάν ο n ισούται με κάποια (θετική ακεραία) δύναμη[21] τού 2.

[21] Η (B.28) δίδει $\varepsilon_2(2^s) = 2^s - 1$ για κάθε $s \in \mathbb{N}$.

Β.4 ΙΣΟΤΙΜΙΕΣ

Β.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[22]

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

όταν $m \mid a-b$. Ο m καλείται, εν προκειμένω, **το μόδιο**[23] τής ισοτιμίας. Όταν $m \nmid a-b$, τότε λέμε ότι ο a είναι **ανισότιμος** τού b κατά μόδιο m και γράφουμε $a \not\equiv b (\mathrm{mod}\, m)$.

Β.4.2 Παρατήρηση. Οι κατωτέρω ιδιότητες τής διμελούς σχέσεως "$\equiv$" (επί τού $\mathbb{Z}$) απορρέουν άμεσα από τον ορισμό Β.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 $a \equiv b (\mathrm{mod}\, n)$.

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

Β.4.3 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

$$a = \kappa m + \nu,\ b = \lambda m + \rho,\ \text{ όπου } \kappa, \lambda, \nu, \rho \in \mathbb{Z} \text{ με } 0 \le \nu, \rho < m.$$

Παρατηρούμε ότι $a \equiv b (\mathrm{mod}\, m) \iff m \mid a-b \iff m \mid \nu - \rho$. Επειδή όμως έχουμε $|\nu - \rho| < m$, βάσει τού Β.1.5 (ii) συμπεραίνουμε ότι $m \mid \nu - \rho \Leftrightarrow \nu = \rho$. □

Β.4.4 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*

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

(ii) *Εάν $a \equiv b (\mathrm{mod}\, m)$, τότε $a \pm c \equiv b \pm c (\mathrm{mod}\, m)$ και $ac \equiv bc (\mathrm{mod}\, m)$.*

(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 $a \equiv b (\mathrm{mod}\, m) \iff ac \equiv bc (\mathrm{mod}\, mc)$.*

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

[22] 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*.

[23] 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.)

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

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

(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 Β.2.14 και το πόρισμα Β.2.9, λαμβάνουμε

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

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 $ac \equiv bc(\mathrm{mod}\, m)$. □

Β.4.5 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 Β.4.4. □

Β.4.6 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 Β.4.5. □

Β.4.7 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 Β.1.5, λαμβάνουμε

$$[m_1 \mid a - b \text{ και } \mu\kappa\delta(m_1, m_2) \mid m_1] \Rightarrow \mu\kappa\delta(m_1, m_2) \mid a - b,$$

και $[m_2 \mid a - c \text{ και } \mu\kappa\delta(m_1, m_2) \mid m_2] \Rightarrow \mu\kappa\delta(m_1, m_2) \mid a - c$. Ως εκ τούτου, λόγω τής ιδιότητας (vi) τής Β.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 $b \equiv c (\mathrm{mod}\, \mu\kappa\delta(m_1, m_2))$. □

Β.4.8 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 Β.2.25) $(m_j \mid a - b,\ \forall j \in \{1, ..., s\}) \Longrightarrow \epsilon\kappa\pi(m_1, ..., m_s) \mid a - b$. Και αντιστρόφως· εάν υποθέσουμε ότι $\epsilon\kappa\pi(m_1, ..., m_s) \mid a - b$ και λάβουμε υπ' όψιν ότι

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

συμπεραίνουμε ότι $a \equiv b (\mathrm{mod}\, m_j)$ για κάθε $j \in \{1, ..., s\}$ (πρβλ. Β.1.5 (v)). □

Β.4.9 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 $a, b \in \mathbb{Z}$. Τότε ισχύει η συνεπαγωγή*

$$[a \equiv b (\mathrm{mod}\, m_j), \forall j \in \{1, ..., s\}] \Longrightarrow a \equiv b\ (\mathrm{mod}\ (\prod_{j=1}^{s} m_j)).$$

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί η πρόταση Β.4.8 και να ληφθεί υπ' όψιν ότι $\epsilon\kappa\pi(m_1, ..., m_s) = \prod_{j=1}^{s} m_j$ (βλ. Β.3.19). □

Β.4.10 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 $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ τον διωνυμικό συντελεστή τού n υπεράνω τού i, όπου $i \in \mathbb{Z}$, $0 \leq i \leq n$. Έστω p ένας πρώτος αριθμός. Τότε*

$$\binom{p}{i} \equiv 0\ (\mathrm{mod}\, p), \quad \forall i \in \{1, ..., p-1\}. \tag{Β.30}$$

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

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

έχουμε

$$\left.\begin{array}{r} p \mid 1\cdot 2\cdot 3\cdots i\cdot \binom{p}{i} \\ \text{μκδ}(p, 1\cdot 2\cdot 3\cdots i) = 1 \end{array}\right\} \underset{\text{B.2.9}}{\Longrightarrow} p \mid \tbinom{p}{i},$$

το οποίο ισοδυναμεί με την ισοτιμία (B.30). □

B.4.11 Πρόταση. *Εάν $a, b \in \mathbb{Z}$ και p είναι πρώτος αριθμός, τότε*

$$(a+b)^p \equiv a^p + b^p (\mathrm{mod}\, p). \tag{B.31}$$

ΑΠΟΔΕΙΞΗ. Κατά τον διωνυμικό τύπο, $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$. Και επειδή ισχύει $\binom{p}{i} \equiv 0 (\mathrm{mod}\, p)$ για κάθε $i \in \{1, ..., p-1\}$ (βλ. λήμμα B.4.10), η ισοτιμία (B.31) είναι αληθής. □

B.4.12 Πόρισμα. *Εάν ο p είναι ένας πρώτος αριθμός, τότε*

$$\boxed{a^p \equiv a (\mathrm{mod}\, p), \ \ \forall a \in \mathbb{Z}.} \tag{B.32}$$

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς παρατηρούμε ότι, όταν $a = 0$ ή $a = 1$, η (B.32) είναι προφανής. Εν συνεχεία αποδεικνύουμε την (B.32) για οιονδήποτε $a \geq 1$ μέσω κλασικής μαθηματικής επαγωγής. Πράγματι· υποθέτοντας ότι η (B.32) είναι αληθής για κάποιον $a \geq 1$, αυτή ισχύει και για τον $a+1$, καθότι

$$\underbrace{\begin{array}{ll} (a+1)^p \equiv a^p + 1 (\mathrm{mod}\, p) & \text{(δυνάμει τής ισοτιμίας (B.31)) και} \\ a^p \equiv a (\mathrm{mod}\, p) & \text{(από την επαγωγική μας υπόθεση)} \end{array}}_{\Downarrow}$$
$$(a+1)^p \equiv a+1 (\mathrm{mod}\, p),$$

πρβλ. B.4.4 (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 B.4.4, 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 (B.32) είναι όντως αληθής *για κάθε* ακέραιο a. □

Β.4.13 Πόρισμα. («Μικρό θεώρημα» τού Fermat, 1640.) *Εάν ο p είναι ένας πρώτος αριθμός και ο a ένας ακέραιος, τέτοιος ώστε*[24] $p \nmid a$, *τότε*[25]

$$\boxed{a^{p-1} \equiv 1 (\mathrm{mod}\, p).} \tag{Β.33}$$

ΑΠΟΔΕΙΞΗ. Προφανής λόγω τής ισοτιμίας (Β.32) και τού πορίσματος Β.4.6 (αφού μκδ$(p, a) = 1$). □

Β.4.14 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 $n = (p-1)^{2k+1}$, $k = 0, 1, 2, ...$ διαπιστώνουμε μέσω τής σχέσεως (Β.33) 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 Β.4.13 (βλ. Β.4.23), 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*.

Β.4.15 Ορισμός. Η απεικόνιση $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ η οριζόμενη μέσω τού τύπου

$$\boxed{\phi(n) := \mathrm{card}\{\, \ell \in \mathbb{N} \mid \ell \leq n \text{ και } \mu\kappa\delta(\ell, n) = 1\}.}$$

καλείται **συνάρτηση φι τού Euler**. Επί παραδείγματι, $\phi(1) = \phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$, $\phi(8) = 4$. Η τιμή $\phi(n)$ τού n μέσω τής ϕ εκφράζεται προφανώς και ως το άθροισμα

$$\boxed{\phi(n) = \sum_{\ell=1}^{n} \left\lfloor \frac{1}{\mu\kappa\delta(\ell, n)} \right\rfloor.} \tag{Β.34}$$

Β.4.16 Λήμμα. *Η συνάρτηση φι τού Euler είναι «πολλαπλασιαστική», ήτοι για $m, n \in \mathbb{N}$ ισχύει η συνεπαγωγή*

$$\mu\kappa\delta(m, n) = 1 \Longrightarrow \phi(mn) = \phi(m)\, \phi(n). \tag{Β.35}$$

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

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

[24] Εξ αυτής τής συνθήκης έπεται, ιδιαιτέρως, ότι $a \neq 0$ (βλ. Β.1.3 (i)).

[25] 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.

και εφαρμόζοντας το πόρισμα Β.2.12 λαμβάνουμε

$$\phi\,(mn) = \text{card}\,(S') = \text{card}\{\,\ell \in S \mid \text{μκδ}\,(\ell, m) = 1 \text{ και } \text{μκδ}\,(\ell, n) = 1\}. \qquad \text{(B.36)}$$

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

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

διαπιστώνουμε ότι κάθε στοιχείο τού S γράφεται μονοσημάντως υπό την μορφή $mq + j$, όπου $0 \le q \le n-1$ και $0 \le j \le m-1$. Βάσει τού (iii) τής προτάσεως Β.2.14, $\text{μκδ}(mq + j, m) = \text{μκδ}(j, m)$, 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 $\phi\,(m)$ 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 $\phi\,(m)$ στηλών υπάρχουν ακριβώς $\phi\,(n)$ αριθμοί, οι οποίοι είναι πρώτοι προς τον n (διότι τότε θα υπάρχουν εν συνόλω $\phi\,(m)\,\phi\,(n)$ 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 $\phi\,(m)$ στήλες, οι οποίες περιέχουν φυσικούς αριθμούς πρώτους προς τον m, είναι οι $j_1, j_2, ..., j_{\phi(m)}$, κι ας θεωρήσουμε το σύνολο

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

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

$$\left.\begin{array}{r} n \mid m(q - \widehat{q}) \\ \text{μκδ}(m, n) = 1 \end{array}\right\} \underset{\text{B.2.9}}{\Longrightarrow} n \mid q - \widehat{q},$$

ήτοι κάτι το άτοπο, αφού $|q - \widehat{q}\,| \le n-1$ (βλ. Β.1.5 (ii)). Κατά συνέπειαν, τα x_q και $x_{\widehat{q}}$ διαιρούμενα διά τού n αφήνουν (σύμφωνα με την πρόταση Β.4.3) *διαφορετικά* υπόλοιπα, οπότε τα n στοιχεία τού S_κ μπορούν να γραφούν υπό τη μορφή

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

όπου $\lambda_0, \lambda_1, ..., \lambda_{n-1}$ είναι κατάλληλοι μη αρνητικοί ακέραιοι αριθμοί. Βάσει τού (iii) τής προτάσεως Β.2.14, $\text{μκδ}(n\lambda_\varrho + \varrho, n) = \text{μκδ}(\varrho, n)$, οπότε

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

Θέτοντας $S'_\kappa := \{\ell \in S_\kappa \mid \text{μκδ}(\ell, mn) = 1\}$ και λαμβάνοντας υπ' όψιν ότι ισχύει $\text{card}(S'_\kappa) = \phi(n)$ για κάθε $\kappa \in \{1, 2, ..., \phi(m)\}$, καθώς και ότι

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

για οιουσδήποτε $\kappa_1, \kappa_2 \in \{1, 2, ..., \phi(m)\}$ με $\kappa_1 \neq \kappa_2$, συμπεραίνουμε ότι

$$S' = \coprod_{\kappa=1}^{\phi(m)} S'_\kappa \Longrightarrow \text{card}(S') = \sum_{\kappa=1}^{\phi(m)} \text{card}(S'_\kappa) = \phi(m)\,\phi(n). \tag{Β.37}$$

Η (Β.37), συνδυαζόμενη με την (Β.36), δίδει τη ζητούμενη ισότητα (Β.35). □

Β.4.17 Θεώρημα. *Εάν $s \in \mathbb{N}$, $s \geq 2$, και εάν οι $m_1, m_2, ..., m_s$ είναι s σχετικώς πρώτοι ανά δύο φυσικοί αριθμοί, τότε*

$$\boxed{\phi\left(\prod_{j=1}^{s} m_j\right) = \prod_{j=1}^{s} \phi(m_j).}$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα κάνοντας χρήση μαθηματικής επαγωγής ως προς το πλήθος s των παραγόντων τού γινομένου και τού λήμματος Β.4.16. □

Β.4.18 Σημείωση. Μια διαφορετική, *αμιγώς ομαδοθεωρητική* απόδειξη τού θεωρήματος Β.4.17 δίδεται στο εδάφιο 7.3.2.

Β.4.19 Λήμμα. *Εάν ο p είναι πρώτος και $k \in \mathbb{N}$, τότε*

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

ΑΠΟΔΕΙΞΗ. Επειδή

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

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

Β.4.20 Πρόταση. *Εάν $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ είναι η κανονική παράσταση* (Β.19) *ενός $n \in \mathbb{N}$, $n \geq 2$, ως γινομένου πρώτων αριθμών, τότε*

$$\boxed{\phi(n) = \prod_{j=1}^{k}\left(p_j^{\alpha_j} - p_j^{\alpha_j - 1}\right) = n\prod_{j=1}^{k}\left(1 - \frac{1}{p_j}\right).} \tag{Β.38}$$

ΑΠΟΔΕΙΞΗ. Από το λήμμα Β.4.16 λαμβάνουμε

$$\begin{aligned} \phi(n) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \phi(p_1^{\alpha_1})\,\phi(p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\ &= \phi(p_1^{\alpha_1})\,\phi(p_2^{\alpha_2})\,\phi(p_3^{\alpha_3} \cdots p_k^{\alpha_k}) = \cdots = \prod_{j=1}^{k} \phi(p_j^{\alpha_j}). \end{aligned}$$

Ως εκ τούτου, από το λήμμα Β.4.19 συνάγεται ότι

$$\prod_{j=1}^{k}\phi\left(p_j^{\alpha_j}\right)=\prod_{j=1}^{k}\left(p_j^{\alpha_j}-p_j^{\alpha_j-1}\right)=\prod_{j=1}^{k}p_j^{\alpha_j}\left(1-p_j^{-1}\right)=n\prod_{j=1}^{k}\left(1-p_j^{-1}\right),$$

απ' όπου έπονται οι τύποι (Β.38) για τη συνάρτηση φι τού Euler. □

Β.4.21 Παράδειγμα. Όταν $n=304920$, ο δεύτερος τύπος εκ των (Β.38) μας παρέχει την τιμή $\phi(n)$ ως ακολούθως:

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

Β.4.22 Πόρισμα. $\phi(d)\mid\phi(n)$, $\forall n\in\mathbb{N}$ *και* $\forall d\in\mathfrak{D}_n$ (βλ. Β.2.34).

ΑΠΟΔΕΙΞΗ. Εάν $n=1$, τότε αυτό είναι προφανές. Εάν $n\geq 2$ και $n=\prod_{j=1}^{k}p_j^{\alpha_j}$ είναι η κανονική παράσταση (Β.19) τού n σε γινόμενο πρώτων παραγόντων, όπου $\alpha_1,\alpha_2,...,\alpha_k\in\mathbb{N}$, τότε

$$d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k},\ \forall d\in\mathfrak{D}_n,$$

όπου $\beta_1,\beta_2,...,\beta_k\in\mathbb{N}_0$ με $0\leq\beta_j\leq\alpha_j$, για κάθε $j\in\{1,...,k\}$ (βλ. Β.3.14). Στην περίπτωση όπου $d=1$, έχουμε προφανώς $\phi(1)=1\mid\phi(n)$. Εάν $d\geq 2$, τότε υπάρχει υποσύνολο δεικτών $\{i_1,...,i_r\}\subseteq\{1,...,k\}$, $r\in\mathbb{N}$, με $\beta_{i_j}>0$ για κάθε $j\in\{1,...,r\}$. Εν τοιαύτη περιπτώσει, θέτοντας $A:=\{p_1,...,p_k\}\smallsetminus\{p_{i_1},...,p_{i_r}\}$ λαμβάνουμε (ύστερα από εφαρμογή τού τύπου (Β.38))

$$\begin{aligned}&\phi(n)=n\left(1-\tfrac{1}{p_1}\right)\cdots\left(1-\tfrac{1}{p_k}\right)\\ &=\left(d\left(1-\tfrac{1}{p_{i_1}}\right)\cdots\left(1-\tfrac{1}{p_{i_r}}\right)\right)\left(\tfrac{n}{d}\prod_{p\in A}\left(1-\tfrac{1}{p}\right)\right)=\phi(d)\left(\tfrac{n}{d}\prod_{p\in A}\left(1-\tfrac{1}{p}\right)\right),\end{aligned}$$

όπου $\prod_{p\in A}\left(1-\frac{1}{p}\right):=1$ όταν $A=\varnothing$. Εάν $A\neq\varnothing$ και $p\in A$, τότε $p\mid\frac{n}{d}$, διότι $p\mid n$ και $p\nmid d$, απ' όπου έπεται ότι $\frac{n}{d}\prod_{p\in A}\left(1-\frac{1}{p}\right)\in\mathbb{N}$ και $\phi(d)\mid\phi(n)$. □

Β.4.23 Θεώρημα. (Θεώρημα τού Euler περί ισοτιμιών) *Έστω* $n\in\mathbb{N}$, $n\geq 2$, *και έστω* a *ένας ακέραιος με* μκδ$(a,n)=1$. *Τότε*

$$\boxed{a^{\phi(n)}\equiv 1(\mathrm{mod}\,n).} \tag{Β.39}$$

ΑΠΟΔΕΙΞΗ. Αρχικώς θα αποδείξουμε μέσω μαθηματικής επαγωγής ότι

$$a^{\phi\left(p^k\right)}\equiv 1(\mathrm{mod}\ p^k) \tag{Β.40}$$

για οιονδήποτε *πρώτο* p, ο οποίος δεν διαιρεί τον a, και για οιονδήποτε φυσικό αριθμό k. Η ισοτιμία (Β.40) είναι αληθής για $k=1$, καθότι εκφράζει την ισοτιμία

(Β.33) τού «μικρού θεωρήματος» τού Fermat. Ας προϋποθέσουμε την ισχύ τής (Β.40) για κάποιον παγιωμένο $k \geq 1$, κι ας γράψουμε τον $a^{\phi\left(p^k\right)}$ ως

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

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

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

Το διωνυμικό ανάπτυγμα, σε συνδυασμό με το λήμμα Β.4.10 και το (iv) τής προτάσεως Β.4.4, μας δίδει

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

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: $a^{\phi\left(p^{k+1}\right)} \equiv 1 (\mathrm{mod}\, p^{k+1})$. Εν συνεχεία, υποθέτοντας ότι μκδ$(n, a) = 1$ και ότι $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ είναι η κανονική παράσταση (Β.19) τού n ως γινομένου πρώτων αριθμών, έχουμε

$$a^{\phi\left(p_j^{\alpha_j}\right)} \equiv 1 (\mathrm{mod}\ p_j^{\alpha_j}),\ \ \forall j \in \{1, ..., s\} \tag{Β.41}$$

(βάσει τού ό,τι έχουμε αποδείξει προηγουμένως). Παρατηρώντας ότι το $\phi(n)$ διαιρείται διά τού $\phi(p_j^{\alpha_j})$ (βάσει τού πορίσματος Β.4.22) έχουμε τη δυνατότητα υψώσεως αμφοτέρων των μελών τής (Β.41) στη δύναμη $\frac{\phi(n)}{\phi\left(p_j^{\alpha_j}\right)}$ (βλ. Β.4.4 (iii)), οπότε λαμβάνουμε

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

Εάν $s = 1$, τότε η (Β.39) 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 Β.4.9 μας δίδει

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

ήτοι την (Β.39). □

Β.4.24 Παράδειγμα. Ας υπολογίσουμε το υπόλοιπο τής διαιρέσεως τού 3^{256} διά τού 100. Επειδή μκδ$(3, 100) = 1$ και

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

η σχέση (4.17) 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.

Β.4.25 Σημείωση. Μια διαφορετική, *αμιγώς ομαδοθεωρητική* απόδειξη τού θεωρήματος Β.4.23 δίδεται στο εδάφιο 4.1.30.

► **Περαιτέρω ιδιότητες τής ϕ και η συνάρτηση μ.** Επειδή η συνάρτηση φι τού Euler χρησιμοποιείται κατά κόρον στη Θεωρία Πεπερασμένων Ομάδων, θα παρατεθούν και κάποιες επιπρόσθετες ιδιότητές της, συμπεριλαμβανομένης τής εκφράσεώς της τη βοηθεία τής συναρτήσεως μι τού Möbius. (Βλ. πρόταση Β.4.34.)

Β.4.26 Πρόταση. *Ο $\phi(n)$ είναι άρτιος για κάθε $n \geq 3$.*

ΑΠΟΔΕΙΞΗ. Εάν $n = \prod_{j=1}^{k} p_j^{\alpha_j}$ είναι η κανονική παράσταση (Β.19) ενός $n \geq 3$ ως γινομένου πρώτων αριθμών, τότε ο τύπος (Β.38) γράφεται ως εξής:

$$\phi(n) = \prod_{j=1}^{k} \left(p_j^{\alpha_j} - p_j^{\alpha_j - 1} \right) = \prod_{j=1}^{k} p_j^{\alpha_j - 1} (p_j - 1). \tag{Β.42}$$

Περίπτωση πρώτη. Εάν ο n είναι *περιττός*, τότε οι $p_1,...,p_k$ είναι κατ' ανάγκην περιττοί και, ως εκ τούτου, οι $p_1 - 1,...,p_k - 1$ άρτιοι. Άρα και ο $\phi(n)$ είναι άρτιος (λόγω τής (Β.42)).

Περίπτωση δεύτερη. Εάν ο n είναι *άρτιος*, τότε $n = 2^\nu m$, για κάποιους $m, \nu \in \mathbb{N}$, όπου ο m είναι περιττός. (Όταν $\nu = 1$, έχουμε $m \geq 3$, διότι εξ υποθέσεως $n \geq 3$.) Συνεπώς,

$$\phi(n) = \begin{cases} 2^{\nu-1}, & \text{όταν } m = 1 \text{ και } \nu \geq 2, \\ 2^{\nu-1}\phi(m), & \text{όταν } m \geq 3 \text{ και } \nu \geq 2, \\ \phi(m), & \text{όταν } m \geq 3 \text{ και } \nu = 1. \end{cases}$$

Στις δύο πρώτες υποπεριπτώσεις ο $\phi(n)$ είναι προδήλως άρτιος. Στην τρίτη υποπερίπτωση, $\phi(n) = \phi(m)$, όπου ο m είναι περιττός και $m \geq 3$, οπότε αρκεί να ληφθούν υπ' όψιν (γι' αυτόν) όσα προαναφέρθησαν στην πρώτη περίπτωση. □

Β.4.27 Πρόταση. $\phi(n) = 2 \iff n \in \{3, 4, 6\}$.

ΑΠΟΔΕΙΞΗ. Επειδή $\phi(1) = \phi(2) = 1$, θεωρούμε τυχόντα φυσικό αριθμό $n \geq 3$. Εάν υποθέσουμε ότι $\phi(n) = 2$, τότε για κάθε πρώτο διαιρέτη p τού n έχουμε (μέσω τού λήμματος Β.4.19 και τού πορίσματος Β.4.22) $\phi(p) = p - 1 \mid 2 (= \phi(n))$, οπότε $p \in \{2, 3\}$. Άρα είτε $n = 2^a$ είτε $n = 2^a \cdot 3^b$ είτε $n = 3^b$, για κάποιους $a, b \in \mathbb{N}$. Στην πρώτη περίπτωση, $a \geq 2$ και $2 = \phi(n) = 2^{a-1}$, οπότε $a = 2$. Στη δεύτερη περίπτωση, $2 = \phi(n) = 2^a \cdot 3^{b-1}$, οπότε $a = b = 1$. Στην τρίτη περίπτωση έχουμε $2 = \phi(n) = 2 \cdot 3^{b-1}$, οπότε $b = 1$. Κατά συνέπειαν, $n \in \{3, 4, 6\}$. (Το αντίστροφο είναι προφανές.) □

Β.4.28 Πρόταση. *Εάν $m, n, \nu \in \mathbb{N}$, και $m \mid n$, τότε $\phi(m^\nu n) = m^\nu \phi(n)$.*

ΑΠΟΔΕΙΞΗ. Εάν $n = 1$, τότε $m = 1$, οπότε η ανωτέρω ισότητα είναι προδήλως αληθής. Εάν $n \geq 2$ και $n = \prod_{j=1}^{k} p_j^{\alpha_j}$ είναι η κανονική παράσταση (Β.19) τού n

ως γινομένου πρώτων αριθμών, τότε (σύμφωνα με το λήμμα Β.3.14) $m=\prod_{j=1}^{k}p_j^{\beta_j}$, όπου $\beta_j\in\{0,1,...,\alpha_j\}$ για κάθε $j\in\{1,...,k\}$, οπότε

$$m^\nu n=\prod_{j=1}^{k}p_j^{\alpha_j+\nu\beta_j}\Rightarrow\phi\left(m^\nu n\right)=m^\nu n\prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right)=m^\nu\phi\left(n\right)$$

επί τη βάσει τού τύπου (Β.38). □

Β.4.29 Πρόταση. *Για οιουσδήποτε $m,n\in\mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\phi\left(mn\right)\phi\left(\text{μκδ}(m,n)\right)=\phi\left(m\right)\phi\left(n\right)\text{μκδ}(m,n).} \tag{Β.43}$$

ΑΠΟΔΕΙΞΗ. Θέτοντας $d:=\text{μκδ}(m,n)$, παρατηρούμε ότι για $d=1$ η (Β.43) είναι η ήδη αποδειχθείσα (Β.35), διότι $\phi\left(1\right)=1$. Ας υποθέσουμε ότι $d\geq 2$. Διακρίνουμε τρεις περιπτώσεις:

Περίπτωση πρώτη. Εάν $m\mid n$, τότε $d=m$ και η (Β.43) είναι αληθής λόγω τής προτάσεως Β.4.28.

Περίπτωση δεύτερη. Παρομοίως, η (Β.43) είναι αληθής όταν $n\mid m$.

Περίπτωση τρίτη. Εάν $m\nmid n$ και $n\nmid m$, και εάν υποτεθεί ότι οι $r_1,...,r_t$ ($t\in\mathbb{N}$) είναι οι (σαφώς διακεκριμένοι για $t>1$) πρώτοι διαιρέτες τού d,τότε οι m,n γράφονται υπό τη μορφή

$$n=\left(\prod_{j=1}^{k}p_j^{\alpha_j}\right)\left(\prod_{s=1}^{t}r_s^{\gamma_s}\right),\ m=\left(\prod_{\varrho=1}^{l}q_\varrho^{\beta_\varrho}\right)\left(\prod_{s=1}^{t}r_s^{\gamma_s}\right),\ \ k,l\in\mathbb{N},$$

όπου $\alpha_1,...,\alpha_k,\beta_1,...,\beta_l,\gamma_1,...,\gamma_t\in\mathbb{N}$, $d=\prod_{s=1}^{t}r_s^{\gamma_s}$ και $p_1,...,p_k,q_1,...,q_l$ πρώτοι αριθμοί (σαφώς διακεκριμένοι, όταν $k>1$ ή/και $l>1$) με

$$\{p_1,...,p_k,q_1,...,q_l\}\cap\{r_1,...,r_t\}=\varnothing.$$

Επομένως, $mn=\left(\prod_{j=1}^{k}p_j^{\alpha_j}\right)\left(\prod_{\varrho=1}^{l}q_\varrho^{\beta_\varrho}\right)\left(\prod_{s=1}^{t}r_s^{2\gamma_s}\right)$,

$$\phi\left(mn\right)=mn\left(\prod_{j=1}^{k}\left(1-\tfrac{1}{p_j}\right)\right)\left(\prod_{\varrho=1}^{l}\left(1-\tfrac{1}{q_\varrho}\right)\right)\left(\prod_{s=1}^{t}\left(1-\tfrac{1}{r_s}\right)\right)$$

(βάσει τού τύπου (Β.38)) και

$$\begin{aligned}\phi\left(mn\right)\phi\left(d\right)&=\phi\left(mn\right)d\prod_{s=1}^{t}\left(1-\tfrac{1}{r_s}\right)\\&=mn\left(\prod_{j=1}^{k}\left(1-\tfrac{1}{p_j}\right)\right)\left(\prod_{\varrho=1}^{l}\left(1-\tfrac{1}{q_\varrho}\right)\right)\left(\prod_{s=1}^{t}\left(1-\tfrac{1}{r_s}\right)\right)^2d\\&=m\left(\prod_{j=1}^{k}\left(1-\tfrac{1}{p_j}\right)\right)\left(\prod_{s=1}^{t}\left(1-\tfrac{1}{r_s}\right)\right)n\left(\prod_{\varrho=1}^{l}\left(1-\tfrac{1}{q_\varrho}\right)\right)\left(\prod_{s=1}^{t}\left(1-\tfrac{1}{r_s}\right)\right)d,\end{aligned}$$

όπου το τελευταίο γινόμενο ισούται με $\phi\left(m\right)\phi\left(n\right)d$. □

Β.4.30 Πόρισμα. *Για οιουσδήποτε $m, n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\phi(m)\,\phi(n) = \phi(\mu\kappa\delta(m,n))\,\phi(\varepsilon\kappa\pi(m,n))\,.} \tag{Β.44}$$

ΑΠΟΔΕΙΞΗ. Κατά την πρόταση Β.4.29,

$$\frac{\phi(m)\,\phi(n)}{\phi(\mu\kappa\delta(m,n))} = \frac{\phi(mn)}{\mu\kappa\delta(m,n)}. \tag{Β.45}$$

Επειδή $mn = \mu\kappa\delta(m,n)\varepsilon\kappa\pi(m,n)$ (βλ. Β.2.29) και

$$[\mu\kappa\delta(m,n) \mid m \text{ και } m \mid \varepsilon\kappa\pi(m,n)] \Rightarrow \mu\kappa\delta(m,n) \mid \varepsilon\kappa\pi(m,n),$$

εφαρμόζοντας την πρόταση Β.4.28 (για $\nu = 1$ και με τους $\mu\kappa\delta(m,n)$ και $\varepsilon\kappa\pi(m,n)$ στη θέση των εκεί παρατεθέντων m και n) λαμβάνουμε

$$\phi(mn) = \phi(\mu\kappa\delta(m,n)\varepsilon\kappa\pi(m,n)) = \mu\kappa\delta(m,n)\phi(\varepsilon\kappa\pi(m,n))\,. \tag{Β.46}$$

Η (Β.44) έπεται άμεσα από τις (Β.45) και (Β.46). □

Β.4.31 Πρόταση. *Για κάθε $n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\sum_{d\in\mathfrak{D}_n} \phi(d) = n.} \tag{Β.47}$$

ΑΠΟΔΕΙΞΗ. Εάν $n = 1$, τότε η (Β.47) είναι προφανής. Εάν $n \geq 2$ και εάν

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ \ k \in \mathbb{N},$$

είναι η κανονική παράσταση (Β.19) τού n ως γινομένου πρώτων αριθμών, τότε (βάσει τού λήμματος Β.3.14) κάθε διαιρέτης $d \in \mathbb{N}$ τού n είναι τής μορφής

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},\ \beta_1,...,\beta_k \in \mathbb{N}_0,\ \beta_j \leq \alpha_j,\ \forall j \in \{1,...,k\},$$

οπότε μέσω τού θεωρήματος Β.4.17 (εφαρμοζόμενου για καθέναν εκ των διαιρετών d τού n) και τού τύπου (Β.38) λαμβάνουμε

$$\sum_{d\in\mathfrak{D}_n} \phi(d) = \sum_{0\leq\beta_1\leq\alpha_1,..,0\leq\beta_k\leq\alpha_k} \phi(p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k})$$

$$= \sum_{0\leq\beta_1\leq\alpha_1,..,0\leq\beta_k\leq\alpha_k} \phi(p_1^{\beta_1})\phi(p_2^{\beta_2}) \cdots \phi(p_k^{\beta_k})$$

$$= \left(\sum_{\beta_1=0}^{\alpha_1} \phi(p_1^{\beta_1})\right)\left(\sum_{\beta_2=0}^{\alpha_2} \phi(p_2^{\beta_2})\right) \cdots \left(\sum_{\beta_k=0}^{\alpha_k} \phi(p_k^{\beta_k})\right) = \prod_{j=1}^{k}\left(\sum_{\beta_j=0}^{\alpha_j} \phi(p_j^{\beta_j})\right)$$

$$= \prod_{j=1}^{k}\Big(1 + (p_j - 1) + (p_j^2 - p_j) + \cdots + (p_j^{\alpha_j} - p_j^{\alpha_j - 1})\Big) = \prod_{j=1}^{k} p_j^{\alpha_j},$$

όπου το τελευταίο γινόμενο είναι το n. □

B.4.32 Ορισμός. Η απεικόνιση $\mu : \mathbb{N} \to \mathbb{N}$ η οριζόμενη μέσω των τύπων $\mu(1) := 1$ και

$$\boxed{\mu(n) := \begin{cases} (-1)^k, & \text{όταν } \alpha_1 = \alpha_2 = \cdots = \alpha_k = 1, \\ 0, & \text{όταν } \exists j \in \{1, ..., k\} : \alpha_j > 1, \end{cases}}$$

όπου $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $k \in \mathbb{N}$, η κανονική παράσταση τού n ως γινομένου πρώτων αριθμών για $n \geq 2$, καλείται **συνάρτηση μι τού Möbius**.

B.4.33 Πρόταση. *Για κάθε $n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\sum_{d \in \mathfrak{D}_n} \mu(d) = \begin{cases} 1, & \text{όταν } n = 1, \\ 0, & \text{όταν } n \geq 2. \end{cases}} \tag{B.48}$$

ΑΠΟΔΕΙΞΗ. Η (B.48) είναι προδήλως αληθής όταν $n = 1$. Ας υποθέσουμε ότι $n \geq 2$ και ότι $n = \prod_{j=1}^{k} p_j^{\alpha_j}$ είναι η κανονική παράσταση (B.19) τού n ως γινομένου πρώτων αριθμών. Εν τοιαύτη περιπτώσει, το πλήθος όλων των θετικών ακεραίων διαιρετών τού n που διαιρούνται διά i εκ των p_1,..., p_k ($i \in \{1, ..., k\}$) και που (ταυτοχρόνως) δεν διαιρούνται διά $p_j^{\beta_j}$, όπου $\beta_j \in \{2,..., \alpha_j\}$ για κάποιον $j \in \{1, ..., k\}$ με $\alpha_j \geq 2$, είναι ίσο με $\binom{k}{i}$. Επομένως,

$$\begin{aligned} \sum_{d \in \mathfrak{D}_n} \mu(d) &= 1 + \sum_{d \in \mathfrak{D}_n \setminus \{1\}} \mu(d) = 1 + \sum_{i=1}^{k} \binom{k}{i} (-1)^i \\ &= \sum_{i=0}^{k} \binom{k}{i} (-1)^i = (1-1)^k = 0 \end{aligned}$$

(από τον δυωνυμικό τύπο). Άρα η (B.48) είναι αληθής και για $n \geq 2$. □

B.4.34 Πρόταση. *Για κάθε $n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\phi(n) = \sum_{d \in \mathfrak{D}_n} \mu(d) \frac{n}{d}.} \tag{B.49}$$

ΑΠΟΔΕΙΞΗ. Εκκινώντας από την (B.34), η (B.48) δίδει

$$\phi(n) = \sum_{\ell=1}^{n} \left\lfloor \frac{1}{\mu\kappa\delta(\ell, n)} \right\rfloor = \sum_{\ell=1}^{n} \left(\sum_{d \in \mathfrak{D}_{\mu\kappa\delta(\ell,n)}} \mu(d) \right) = \sum_{\ell=1}^{n} \left(\sum_{d \in \mathfrak{D}_n, d \in \mathfrak{D}_\ell} \mu(d) \right).$$

Για κάθε παγιωμένον $d \in \mathfrak{D}_n$ η άθροιση περιλαμβάνει όλους τους $\ell \in \{1, ..., n\}$ για τους οποίους υπάρχει κάποιος $j \in \mathbb{N}$ με $\ell = jd$. Επομένως, $1 \leq j \leq \frac{n}{d}$ και

$$\phi(n) = \sum_{d \in \mathfrak{D}_n} \left(\sum_{j=1}^{\frac{n}{d}} \mu(d) \right) = \sum_{d \in \mathfrak{D}_n} \mu(d) \left(\sum_{j=1}^{\frac{n}{d}} 1 \right) = \sum_{d \in \mathfrak{D}_n} \mu(d) \frac{n}{d},$$

οπότε η ισότητα (Β.49) είναι αληθής. □

► **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 $\mathbb{Z}$.

Β.4.35 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 διμελής σχέση "$\sim_m$" είναι αυτοπαθής, διότι $a - a = 0 = 0 \cdot m$, συμμετρική, διότι $a - b = km \Rightarrow b - a = (-k)\, m$, και μεταβατική λόγω τής συνεπαγωγής

$$[a - b = k_1 m \ \text{ και } \ b - c = k_2 m] \Rightarrow a - c = (k_1 + k_2)\, m,$$

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 $a \equiv c (\mathrm{mod}\, m)$. □

Β.4.36 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

$$..., [-2]_m, [-1]_m, [0]_m, [1]_m, [2]_m, ...$$

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).

Β.4.37 Πρόταση. *Το ανωτέρω σύνολο των κλάσεων υπολοίπων γράφεται σε «ανηγμένη» μορφή* [26] *ως ακολούθως:*

$$\boxed{\mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}.} \tag{Β.50}$$

[26] 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. (Β.1)), λαμβάνουμε την ισότητα $[a]_m = [r]_m$. Εξ αυτού συνάγεται ότι οι *σαφώς διακεκριμένες* κλάσεις ισοδυναμίας που διαθέτουμε είναι οι μόνον οι $[0]_m, [1]_m, ..., [m-1]_m$. □

Β.4.38 Σημείωση. Χρησιμοποιώντας τήν ορολογία που εισήχθη στο Α.1.12 διαπιστώνουμε μέσω τής προτάσεως Β.4.37 ότι το σύνολο $\{0, 1, ..., m-1\}$ είναι ένα *πλήρες σύστημα εκπροσώπων*[27] *τού* $\mathbb{Z}$ *ως προς την* "$\sim_m$" , οπότε

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

Προσοχή! Για κάθε $j \in \{0, 1, ..., m-1\}$ 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.

Β.4.39 Παραδείγματα. (i) Πέραν τού $\{0, 1, ..., m-1\}$, *και* τα $\{1, ..., m\}$ και

$$\left\{ \begin{array}{ll} \left\{ -\left(\frac{m}{2} - 1\right), ..., -1, 0, 1, ..., \frac{m}{2} \right\}, & \text{όταν } m \equiv 0 (\mathrm{mod}\, 2) \\ \left\{ -\frac{m-1}{2}, ..., -1, 0, 1, ..., \frac{m-1}{2} \right\}, & \text{όταν } m \equiv 1 (\mathrm{mod}\, 2) \end{array} \right\}$$

αποτελούν «φυσικώς κατασκευαζόμενα» πλήρη συστήματα εκπροσώπων τού $\mathbb{Z}$ ως προς την "$\sim_m$".

(ii) Το $\{14, 24, 9, -11, 34, 68, -21, 87\}$ αποτελεί ένα πλήρες σύστημα εκπροσώπων τού $\mathbb{Z}$ ως προς την "$\sim_8$", διότι

$$\begin{array}{llll} 24 \equiv 0 (\mathrm{mod}\, 8), & 9 \equiv 1 (\mathrm{mod}\, 8), & 34 \equiv 2 (\mathrm{mod}\, 8), & -21 \equiv 3 (\mathrm{mod}\, 8), \\ 68 \equiv 4 (\mathrm{mod}\, 8), & -11 \equiv 5 (\mathrm{mod}\, 8), & 14 \equiv 6 (\mathrm{mod}\, 8), & 87 \equiv 7 (\mathrm{mod}\, 8). \end{array}$$

(iii) Όταν $m \geq 3$, το $\{1, 2^2, 3^2, ..., m^2\}$ δεν αποτελεί ένα πλήρες (παρά μόνον ένα *μερικό*) σύστημα εκπροσώπων τού $\mathbb{Z}$ ως προς την "$\sim_m$", διότι προφανώς ισχύει $(m-1)^2 - 1 = m(m-2)$, οπότε $(m-1)^2 \equiv 1 (\mathrm{mod}\, m)$.

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

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

(*προσθέσεως* και *πολλαπλασιασμού*, αντιστοίχως) μέσω των τύπων

$$\boxed{\begin{array}{c} [a]_m +_{\mathbb{Z}_m} [b]_m := [a+b]_m, \\ [a]_m \cdot_{\mathbb{Z}_m} [b]_m := [ab]_m. \end{array}} \tag{Β.51}$$

[27] 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 $a_j \equiv j (\mathrm{mod}\, m)$, $\forall j \in \{0, 1, ..., m-1\}$.

Β.4.40 Σημείωση. (i) Η απόδειξη τού ότι οι "$+_{\mathbb{Z}_m}$" και "$\cdot_{\mathbb{Z}_m}$" είναι *καλώς ορισμένες* πράξεις μέσω των τύπων (Β.51), ήτοι τού ότι ισχύει η συνεπαγωγή

$$\left.\begin{array}{c}[a]_m=[a']_m\\ [b]_m=[b']_m\end{array}\right\}\Rightarrow\left\{\begin{array}{c}[a]_m+_{\mathbb{Z}_m}[b]_m=[a']_m+_{\mathbb{Z}_m}[b']_m\\ \text{και } [a]_m\cdot_{\mathbb{Z}_m}[b]_m=[a']_m\cdot_{\mathbb{Z}_m}[b']_m\end{array}\right\},$$

είναι εύκολη και αφήνεται ως άσκηση.

(ii) Επειδή κατά την εφαρμογή των ορισμών (Β.51) 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 (Β.50) 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:

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

Οι κύριες ιδιότητες των πράξεων "$+_{\mathbb{Z}_m}$" και "$\cdot_{\mathbb{Z}_m}$" περιγράφονται στις προτάσεις Β.4.41 και Β.4.42. (Οι αποδείξεις τους βασίζονται στις γνωστές ιδιότητες τής προσθέσεως και τού πολλαπλασιασμού ακεραίων, και αφήνονται ως άσκηση.)

Β.4.41 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. 1.2.6), *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. 1.2.11), *δηλαδή*

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

Β.4.42 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. 1.2.6), *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*

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

Β.4.43 Πρόταση. *Ένα στοιχείο* $[a]_m$ *τού* $\mathbb{Z}_m$ *διαθέτει αντίστροφο (ήτοι συμμετρικό στοιχείο*[28]*) ως προς την* "$\cdot_{\mathbb{Z}_m}$" *εάν και μόνον εάν* $\text{μκδ}(a, m) = 1$.

ΑΠΟΔΕΙΞΗ. Έστω ότι το $[a]_m$ διαθέτει το $[b]_m$ ως αντίστροφό του στοιχείο ως προς την "$\cdot_{\mathbb{Z}_m}$". Τότε $[a]_m \cdot_{\mathbb{Z}_m} [b]_m = [ab]_m = [1]_m \Rightarrow \exists k \in \mathbb{Z} : ab = mk + 1$. Τούτο, σύμφωνα με το πόρισμα Β.2.8, σημαίνει ότι $\text{μκδ}(a, m) = 1$. Και αντιστρόφως· υποθέτοντας ότι $\text{μκδ}(a, m) = 1$, θα υπάρχουν $c, d \in \mathbb{Z}$, τέτοιοι ώστε

$$\begin{aligned} &ac + md = 1 \Rightarrow [ac + md]_m = ([a]_m \cdot_{\mathbb{Z}_m} [c]_m) +_{\mathbb{Z}_m} ([m]_m \cdot_{\mathbb{Z}_m} [d]_m) = [1]_m \\ &\Longrightarrow ([a]_m \cdot_{\mathbb{Z}_m} [c]_m) = [1]_m \ \text{(λόγω τού Β.4.42 (iii) και τού ότι } [m]_m = [0]_m), \end{aligned}$$

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

[28] 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 1.2.13. Εξάλλου, επειδή η "$\cdot_{\mathbb{Z}_m}$" είναι μεταθετική (βλ. Β.4.42 (i)), αρκεί κανείς να περιορισθεί στην εξέταση υπάρξεως εκ δεξιών συμμετρικού στοιχείου τού $[a]_m$ (βλ. 1.2.14).

Β.4.44 Σημείωση. (Απλούστευση συμβολισμών) Υιοθετώντας, για λόγους χρηστικότητας, την «ελάφρυνση» των συμβολισμών των πράξεών μας, 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 $m\in\mathbb{N}$ και $a,b\in\mathbb{Z}$. Κάθε ισοτιμία τής μορφής

$$\boxed{ax\equiv b(\mathrm{mod}\, m),} \tag{B.52}$$

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 (Β.52) 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 (Β.52). 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** (Β.52) **κατά μόδιο** m, εννοούμε ολόκληρη[29] την κλάση $[x_0]_m$, όπου ο x_0 πληροί την (Β.52). 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 Β.4.37 προτιμούμε να παραθέτουμε τον *μοναδικό* εκπρόσωπο x_0' τής κλάσεως υπολοίπων $[x_0]_m$ ο οποίος ανήκει στο σύνολο $\{0,1,...,m-1\}$, ήτοι να καταφεύγουμε σε *αναγωγή* τού x_0 κατά μόδιο m κατόπιν διαιρέσεώς του διά τού m (βλ. απόδειξη τής Β.4.37).

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 (Β.52) και, επιπροσθέτως, περιγράφει τη μορφή όλων των δυνατών λύσεων.

Β.4.45 Πρόταση. *Δοθέντων ενός $m\in\mathbb{N}$ και δυο ακεραίων a,b, $a\neq 0$, η γραμμική ισοτιμία* (Β.52) *διαθέτει λύσεις $x\in\mathbb{Z}$ κατά μόδιο m εάν και μόνον εάν* $\mathrm{μκδ}\,(a,m)\,|\,b$. *Επιπροσθέτως, όταν* $\mathrm{μκδ}\,(a,m)\,|\,b$, *η ισοτιμία* (Β.52) *διαθέτει ακριβώς* $\mathrm{μκδ}(a,m)$ *σαφώς διακεκριμένες λύσεις $x\in\mathbb{Z}$ κατά μόδιο m, οι οποίες είναι τής μορφής*

$$\boxed{x=x_0+k\,\frac{m}{\mathrm{μκδ}\,(a,m)},\quad k\in\{0,1,...,\mathrm{μκδ}\,(a,m)-1\},} \tag{B.53}$$

όπου x_0 μια ειδική λύση τής (Β.52).

ΑΠΟΔΕΙΞΗ. Εάν η (Β.52) δέχεται μια λύση $x\in\mathbb{Z}$ κατά μόδιο m, τότε

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

Επομένως,

$$\left.\begin{array}{r}\mathrm{μκδ}\,(a,m)\mid a\\ \mathrm{μκδ}\,(a,m)\mid m\end{array}\right\}\underset{\text{(βλ. Β.1.5 (vi))}}{\Longrightarrow}\mathrm{μκδ}\,(a,m)\mid ax-km\,(=b).$$

[29] Γι' αυτόν τον λόγο, δυο ακέραιες λύσεις x_1 και x_2 τής (Β.52) λογίζονται ως *διαφορετικές* όταν $x_1\not\equiv x_2(\mathrm{mod}\, m)$.

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 Β.2.14, ισχύει η

$$\text{μκδ}\left(\tfrac{a}{\text{μκδ}(a,m)}, \tfrac{m}{\text{μκδ}(a,m)}\right) = 1 \underset{\text{(βλ. Β.2.8)}}{\Longrightarrow} \left(\exists \kappa, \lambda \in \mathbb{Z} : \kappa \tfrac{a}{\text{μκδ}(a,m)} + \lambda \tfrac{m}{\text{μκδ}(a,m)} = 1\right),$$

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 (Β.52).

Εν συνεχεία υποθέτουμε οτι το x_0 (ή, ακριβέστερα, η κλάση $[x_0]_m$) είναι μια παγιωμένη (ειδική) λύση τής (Β.52). 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 (Β.53) αποτελούν πράγματι λύσεις τής (Β.52). Οι ακέραιοι αυτοί είναι ανά δύο ανισότιμοι κατά μόδιο m, καθότι για οιουσδήποτε ακεραίους αριθμούς $k, k' \in \{0, 1, ..., \text{μκδ}(a,m) - 1\}$ 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 Β.1.5, έχουμε

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

Απομένει λοιπόν να αποδειχθεί ότι και κάθε άλλη λύση $y \in \mathbb{Z}$ τής (Β.52) είναι ισότιμη με κάποια εκ των (Β.53) κατά μόδιο m. Επειδή

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

συμπεραίνουμε ότι

$$\left.\begin{aligned} \tfrac{m}{\text{μκδ}(a,m)} &\mid \tfrac{a}{\text{μκδ}(a,m)}\,(y - x_0) \\ \text{μκδ}\left(\tfrac{a}{\text{μκδ}(a,m)}, \tfrac{m}{\text{μκδ}(a,m)}\right) &= 1 \end{aligned}\right\} \Longrightarrow \begin{gathered} \tfrac{m}{\text{μκδ}(a,m)} \mid y - x_0 \\ \Downarrow \\ \left(\exists \nu \in \mathbb{Z} : y - x_0 = \tfrac{m\nu}{\text{μκδ}(a,m)}\right). \end{gathered}$$

Διαιρώντας τον ν διά τού $\text{μκδ}(a,m)$ λαμβάνουμε ένα μονοσημάντως ορισμένο ζεύγος $(q, r) \in \mathbb{Z}^2$ με $\nu = \text{μκδ}(a,m)\, q + r,\ 0 \leq r \leq \text{μκδ}(a,m) - 1$. Ως εκ τούτου,

$$y - x_0 = \tfrac{m(\text{μκδ}(a,m)q + r)}{\text{μκδ}(a,m)} = mq + \tfrac{rm}{\text{μκδ}(a,m)} \equiv \tfrac{rm}{\text{μκδ}(a,m)} (\text{mod } m),$$

οπότε $y \equiv x_0 + r\tfrac{m}{\text{μκδ}(a,m)} (\text{mod } m)$, $\forall r \in \{0, 1, ..., \text{μκδ}(a,m) - 1\}$. □

Β.4.46 Παρατήρηση. (i) Αντί τού $k \in \{0,1,...,$ μκδ$(a,m)-1\}$ μπορούμε στην (Β.53) (επειδή εργαζόμαστε $\bmod m$) να γράψουμε $k \in \{1,...,$ μκδ$(a,m)\}$.
(ii) Όταν $b=0$, τότε θέτουμε $x_0 := 0$.

Β.4.47 Πόρισμα. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a,b, $a \neq 0$, η γραμμική ισοτιμία* (Β.52) *διαθέτει ακριβώς μία λύση x_0 κατά μόδιο m εάν και μόνον εάν* μκδ $(a,m)=1$.

Β.4.48 Σημείωση. Όταν μκδ$(a,m)=1$, 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 Β.2.21). Ένας άλλος τρόπος υπολογισμού τής λύσεως x_0 είναι δυνατός κατόπιν εφαρμογής τού θεωρήματος Β.4.23 τού Euler περί ισοτιμιών. Σύμφωνα με αυτό, (λόγω τής συνθήκης μκδ$(a,m)=1$) έχουμε $a^{\phi(m)} \equiv 1 (\bmod m)$, όπου ϕ η συνάρτηση φι τού Euler (βλ. Β.4.15). Ως εκ τούτου, αρκεί να θέσουμε

$$\boxed{x_0 := a^{\phi(m)-1} b,} \tag{Β.54}$$

να εφαρμόσουμε τον τύπο (Β.38) για την εύρεση τού $\phi(m)$ για τον δοθέντα φυσικό αριθμό m και να διενεργήσουμε αναγωγή κατά μόδιο m.

Β.4.49 Παράδειγμα. Επειδή μκδ$(5,24)=1$, η γραμμική ισοτιμία $5x \equiv 3 (\bmod 24)$ διαθέτει ακριβώς μία λύση x_0 κατά μόδιο m. Γράφοντας $24 = 2^3 \cdot 3$, ο τύπος (Β.38) μας δίδει την τιμή $\phi(24) = (2^3 - 2^2)(3-1) = 8$. Κατά τον (Β.54), 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 $5 \cdot 15 \equiv 3 (\bmod 24)$.

Η εύρεση των λύσεων τής γενικής γραμμικής ισοτιμίας (Β.52) ανάγεται -κατ' ουσίαν- στην ειδική περίπτωση που περιγράψαμε στα Β.4.47 και Β.4.48, ως ακολούθως:

Β.4.50 Πόρισμα. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a,b, $a \neq 0$, με* μκδ $(a,m) \mid b$, *η γραμμική ισοτιμία* (Β.52) *διαθέτει* μκδ(a,m) *λύσεις $x \in \mathbb{Z}$ κατά μόδιο m, οι οποίες είναι τής μορφής* (Β.53), *όπου x_0 η μοναδική λύση κατά μόδιο $\frac{m}{\text{μκδ}(a,m)}$ τής*

$$\left(\tfrac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\tfrac{b}{\text{μκδ}(a,m)}\right) (\bmod \ \left(\tfrac{m}{\text{μκδ}(a,m)}\right)). \tag{Β.55}$$

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. Β.2.14 (ii)), καθώς και τις ακόλουθες αμφίπλευρες συνεπαγωγές:

$$ax \equiv b (\bmod \ m) \quad \Leftrightarrow \text{μκδ}\,(a,m)\,\widetilde{a}x \equiv \text{μκδ}\,(a,m)\,\widetilde{b} \,(\bmod \text{μκδ}\,(a,m)\,\widetilde{m})$$
$$\Leftrightarrow \widetilde{a}x \equiv \widetilde{b} \,(\bmod \ \widetilde{m}) \Leftrightarrow \left(\tfrac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\tfrac{b}{\text{μκδ}(a,m)}\right) \ (\bmod \ \left(\tfrac{m}{\text{μκδ}(a,m)}\right)),$$

διότι μκδ$(a,m) \neq 0$ (βλ. Β.4.4 (iv)), οπότε η (Β.55) ισοδυναμεί με την (Β.52). □

Β.4.51 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 Β.4.50 το x_0 είναι η μοναδική λύση τής $2x \equiv 1 (\mathrm{mod}\ 7)$ κατά μόδιο 7. Εφαρμόζοντας τον τύπο (Β.54) θέτουμε

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

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

Κλείνουμε το παρόν παράρτημα παραθέτοντας μια απλή ικανή και αναγκαία συνθήκη[30], ούτως ώστε ένας ακέραιος > 1 να είναι *πρώτος*.

Β.4.52 Θεώρημα. (J. Wilson) *Ένας ακέραιος $p > 1$ είναι πρώτος εάν και μόνον εάν*[31]

$$\boxed{(p-1)! \equiv -1 \,(\mathrm{mod}\ p)\,.} \tag{Β.56}$$

ΑΠΟΔΕΙΞΗ. Έστω p ένας πρώτος αριθμός. Εάν $p = 2$ ή $p = 3$, τότε η (Β.56) είναι προφανώς αληθής. Εάν ο p είναι πρώτος ≥ 5, θεωρούμε ένα $a \in \{1, 2, ..., p-1\}$ και τη γραμμική ισοτιμία $ax \equiv 1 \,(\mathrm{mod}\ p)$. 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 $aa' \equiv 1 \,(\mathrm{mod}\ p)$. Επειδή ο p είναι πρώτος, έχουμε

$$a = a' \Longleftrightarrow (\text{είτε } \ a = 1 \ \text{ είτε } \ a = p-1)\,. \tag{Β.57}$$

Πράγματι· από την ισοτιμία $a^2 \equiv 1 \,(\mathrm{mod}\ p)$ συνάγεται 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 "$\Rightarrow$" τής (Β.57), αφού έχουμε $1 \leq a \leq p-1$ και $1 \leq a' \leq p-1$. Και αντιστρόφως· εάν $a = 1$, τότε

$$\left.\begin{array}{r} a' \equiv 1 \,(\mathrm{mod}\ p) \Longrightarrow p \mid a'-1 \\ 1 \leq a' \leq p-1 \end{array}\right\} \underset{\text{(βλ. Β.1.5 (ii))}}{\Longrightarrow} a'-1 = 0 \Longrightarrow a' = 1,$$

[30] Παρά το γεγονός ότι η (Β.56) αποτελεί μια ικανή και αναγκαία συνθήκη για να είναι ένας ακέραιος $p > 1$ πρώτος, είναι πρακτικώς μη αποδοτική για τον προσδιορισμό *μεγάλων πρώτων*, καθόσον εμπεριέχει το παραγοντικό. Για μια πρώτη γνωριμία με αποδοτικούς αλγορίθμους ευρέσεως πρώτων ή ελέγχου τού κατά πόσον κάποιος φυσικός αριθμός είναι πρώτος, οι ενδιαφερόμενοι αναγνώστες παραπέμπονται στο βιβλίο τού D.M. Bressoud: *Factorization and Primality Testing*, UTM, Springer-Verlag, 1989, καθώς και στα τρία βιβλία τού P. Ribenboim:
The Book of Prime Number Records, second. ed., Springer-Verlag, 1989.
The Little Book of Big Primes, Springer-Verlag, 1991.
The Little Book of Bigger Primes, second. ed., Springer-Verlag, 2004.

[31] 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 (Β.56). 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.

και εάν $a = p - 1$, τότε

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

οπότε

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

και, ως εκ τούτου,

$$\left.\begin{array}{r} p \equiv a' + 1 \,(\mathrm{mod}\ p) \Longrightarrow p \mid p - (a'+1) \\ 0 \leq p - (a'+1) \leq p - 2 \end{array}\right\} \underset{(\beta\lambda.\ \mathrm{B.1.5\ (ii)})}{\Longrightarrow} a' = p - 1,$$

και η συνεπαγωγή "$\Leftarrow$" τής (B.57) είναι όντως αληθής. Ομαδοποιούμε, εν συνεχεία, τους εναπομένοντες φυσικούς αριθμούς

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

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

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

Επειδή $p - 1 \equiv -1 \,(\mathrm{mod}\ p)$, η (B.56) προκύπτει από το B.1.5 (v).

Αντιστρόφως τώρα· υποθέτοντας ότι

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

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. □

B.4.53 Σημείωση. Για μια διαφορετική, *ομαδοθεωρητική* απόδειξη τού θεωρήματος B.4.52 βλ. άσκηση **2-42**.