ΚΕΦΑΛΑΙΟ 5

Θεωρία διαιρετότητας σε ακέραιες περιοχές

Στο πλαίσιο τής Στοιχειώδους Θεωρίας Αριθμών έχουμε μελετήσει τις *ιδιότητες τής διαιρετότητας ακεραίων αριθμών*, τον τρόπο εκτελέσεως τού *ευκλειδείου αλγορίθμου διαιρέσεως*, έχουμε ορίσει τις έννοιες *μέγιστος κοινός διαιρέτης* και *ελάχιστο κοινό πολλαπλάσιο*, και έχουμε αποδείξει ότι κάθε $a \in \mathbb{Z}\setminus\{0, \pm 1\}$ παριστάται ως γινόμενο

$$a = \text{sign}(a) p_1^{\nu_1} p_2^{\nu_2} \cdots p_k^{\nu_k},$$

όπου $\text{sign}(a)$ είναι ο προσημασμένος άσος τού a, ήτοι

$$\text{sign}(a) := \begin{cases} 1, & \text{όταν } a > 0, \\ -1, & \text{όταν } a < 0, \end{cases}$$

$k \in \mathbb{N}$, $p_1, \ldots, p_k$ κατάλληλοι σαφώς διακεκριμένοι *πρώτοι αριθμοί* υψούμενοι σε θετικές ακέραιες δυνάμεις $\nu_1, \ldots, \nu_k$. (Η παράσταση αυτή είναι *μονοσημάντως ορισμένη*, μη λαμβανομένης υπ' όψιν τής διατάξεως των πρώτων αριθμών $p_1, \ldots, p_k$, για κάθε $a \in \mathbb{Z}\setminus\{0, \pm 1\}$.)

Σκοπός τού παρόντος κεφαλαίου είναι να εξηγήσει το πώς γενικεύονται τα ανωτέρω (που αφορούν στον δακτύλιο $\mathbb{Z}$) σε *τυχούσες ακέραιες περιοχές*. Οι προσήκουσες εννοιολογικές γενικεύσεις, οι οποίες θα εισαχθούν, θα οδηγήσουν στην *ιεράρχηση* των ακεραίων περιοχών επί τη βάσει τής διατηρήσεως ή τής μη διατηρήσεως των θεμελιωδών αριθμοθεωρητικών ή δακτυλιοθεωρητικών ιδιοτήτων τού $\mathbb{Z}$ που οφείλονται -κατά κύριο λόγο- στη *διαιρετότητα*.

5.1 ΑΡΧΙΚΕΣ ΕΠΙΣΗΜΑΝΣΕΙΣ

► **Ευκλείδεια διαίρεση**. Ήδη από τα γραφόμενα στο βιβλίο VII των ευκλειδείων «Στοιχείων» συνάγεται το ακόλουθο:

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

$$\boxed{a = qb + r, \text{ όπου } 0 \leq r < |b|\,.} \tag{5.1}$$

Τα q *και* r *στην* (5.1) *είναι το* ***πηλίκο*** *και, αντιστοίχως, το* ***υπόλοιπο*** *τής διαιρέσεως τού* a *διά τού* b.

5.1.2 Σημείωση. Οι ακέραιες περιοχές στις οποίες ορίζεται «ευκλείδεια διαίρεση» (υπό μία κατά τι γενικότερη έννοια) ως προς κάποια «ευκλείδεια στάθμη», καλούνται *ευκλείδειες περιοχές*. (Βλ. τον καταλλήλως τροποποιούμενο ορισμό 5.4.1.) Επισημαίνεται ότι, εν προκειμένω, δεν προαπαιτείται η μοναδικότητα των εμφανιζομένων πηλίκων και υπολοίπων (βλ. 5.4.2 (ii), 5.4.18 και 5.4.19 (ii)). Οι ευκλείδειες περιοχές αποτελούν μια *πολύ ειδική υποκλάση* τής κλάσεως των περιοχών κυρίων ιδεωδών. (Βλ. θεώρημα 5.4.21.)

► **Μέγιστος κοινός διαιρέτης**. Εάν $a, b \in \mathbb{Z}$, τότε, ως συνήθως, γράφουμε $a \mid b$ για να υποδηλώσουμε ότι ο a είναι *διαιρέτης τού* b, δηλαδή ότι υπάρχει κάποιος $c \in \mathbb{Z}$ με $b = ac$. Εάν $n \in \mathbb{N},\ n \geq 2$, και εάν οι $a_1, \ldots, a_n$ είναι ακέραιοι αριθμοί με έναν τουλάχιστον εξ αυτών $\neq 0$, τότε το σύνολο $\mathcal{S}$ των θετικών κοινών διαιρετών τους είναι μη κενό, καθότι $1 \in \mathcal{S}$. Επειδή $a_k \neq 0$ για κάποιον $k \in \{1, ..., n\}$, έχουμε $c \mid a_k$ και, ως εκ τούτου, $c \leq |a_k|$, για οιοδήποτε στοιχείο c τού $\mathcal{S}$. Κατά συνέπειαν, το $\mathcal{S}$ είναι πεπερασμένο. Το μέγιστο στοιχείο τού συνόλου $\mathcal{S}$ (ως προς την " $\leq$ ") είναι ο *μέγιστος κοινός διαιρέτης* των $a_1, \ldots, a_n$ που τον συμβολίζουμε, ως συνήθως, ως μκδ$(a_1, \ldots, a_n)$. Σημειωτέον ότι για κάθε $a \in \mathbb{Z}$ το σύνολο των θετικών διαιρετών τού a συμπίπτει με το σύνολο των θετικών διαιρετών τού $-a$. Επομένως,

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

δηλαδή ο μκδ των $a_1, \ldots, a_n$ είναι *ανεξάρτητος* των προσήμων τους. Επίσης, επειδή $a \mid 0,\ \forall a \in \mathbb{Z}$, έχουμε μκδ$(0, a_1, \ldots, a_n) =$ μκδ$(a_1, \ldots, a_n)$. (Σύμβαση: Είναι δυνατή η επέκταση τής εννοίας τού μεγίστου κοινού διαιρέτη ακόμη και όταν $a_1 = \cdots = a_n = 0$. Εν τοιαύτη περιπτώσει, θέτουμε μκδ$(0, \ldots, 0) := 0$.)

5.1.3 Πρόταση. *Εάν* $n \in \mathbb{N},\ n \geq 2$, *και* $a_1, \ldots, a_n \in \mathbb{Z}$, *τότε ένας* $d \in \mathbb{N}_0$ *ισούται με τον* μκδ$(a_1, \ldots, a_n)$ *εάν και μόνον εάν ισχύουν τα ακόλουθα*:

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

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

5.1.4 Σημείωση. (i) Στον αρχικό ορισμό τού μεγίστου κοινού διαιρέτη μκδ$(a_1, \ldots, a_n)$ (όταν τουλάχιστον ένας εκ των $a_1, \ldots, a_n$ είναι $\neq 0$) υπεισέρχεται κατά τρόπο ουσιαστικό η συνήθης διάταξη " $\leq$ " των ακεραίων αριθμών. Γι' αυτόν τον λόγο, για να γενικευθεί η έννοια τού μεγίστου κοινού διαιρέτη σε *τυχούσες* ακέραιες περιοχές που δεν είναι κατ' ανάγκην εφοδιασμένες με κάποια σχέση διατάξεως (με το επίθετο *μέγιστος* υπενθυμίζον απλώς την *προέλευση* τού όρου) χρησιμοποιείται μια ελαφρά παραλλαγή[1] τής ανωτέρω προτάσεως 5.1.3 (βλ. ορισμό 5.2.9). Ωστόσο, είναι απαραίτητο να τονισθεί ότι, εν τοιαύτη περιπτώσει, δεν πρέπει να θεωρείται εν γένει ως δεδομένη *ούτε η ύπαρξη* (τέτοιων γενικευμένων) μεγίστων κοινών διαιρετών *ούτε η μοναδικότητά τους* (όταν υπάρχουν).

(ii) Ως γνωστόν, μέσω τής εκτελέσεως πεπερασμένου πλήθους ευκλειδείων διαιρέσεων είναι δυνατός ο προσδιορισμός τού μεγίστου κοινού διαιρέτη μκδ(a, b) οιωνδήποτε $a, b \in \mathbb{Z} \setminus \{0\}$. Τούτο γενικεύεται καταλλήλως και για οιαδήποτε ευκλείδεια περιοχή. (Βλ. πρόταση 5.4.28.)

► **Ελάχιστο κοινό πολλαπλάσιο.** Έστω ότι $n \in \mathbb{N},\ n \geq 2$, και ότι οι $a_1, \ldots, a_n$ είναι μη μηδενικοί ακέραιοι αριθμοί. Προφανώς ο φυσικός αριθμός $|a_1 \cdots a_n|$ είναι ένα κοινό πολλαπλάσιο των $a_1, \ldots, a_n$. Ως εκ τούτου, το σύνολο των θετικών πολλαπλασίων των $a_1, \ldots, a_n$ είναι μη κενό και διαθέτει ένα (και μόνον) *ελάχιστο* στοιχείο. Το στοιχείο αυτό είναι το *ελάχιστο κοινό πολλαπλάσιο* των $a_1, \ldots, a_n$ που το συμβολίζουμε, ως συνήθως, ως εκπ$(a_1, \ldots, a_n)$. Επειδή το σύνολο των θετικών πολλαπλασίων των $a_1, \ldots, a_n$ ισούται με το σύνολο των θετικών πολλαπλασίων των $|a_1|, \ldots, |a_n|$, συμπεραίνουμε ότι εκπ$(a_1, \ldots, a_n) =$ εκπ$(|a_1|, \ldots, |a_n|)$. (Σύμβαση: Είναι δυνατή η επέκταση τής εννοίας τού ελαχίστου κοινού πολλαπλασίου ακόμη και όταν τουλάχιστον ένας εκ των $a_1, \ldots, a_n$ είναι $= 0$. Εν τοιαύτη περιπτώσει, θέτουμε εκπ$(a_1, \ldots, a_n) := 0$.)

5.1.5 Πρόταση. *Εάν* $n \in \mathbb{N},\ n \geq 2$*, και* $a_1, \ldots, a_n \in \mathbb{Z}$*, τότε ένας* $t \in \mathbb{N}_0$ *ισούται με το* εκπ$(a_1, \ldots, a_n)$ *εάν και μόνον εάν ισχύουν τα ακόλουθα*:

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

(ii) *για οιονδήποτε* $s \in \mathbb{Z}$*, για τον οποίο ισχύει* $a_1 \mid s, \ldots, a_n \mid s$*, έχουμε* $t \mid s$.

5.1.6 Σημείωση. Κατ' αναλογίαν προς τα προαναφερθέντα στο εδάφιο 5.1.4 (i), για να γενικευθεί η έννοια τού ελαχίστου κοινού πολλαπλασίου σε *τυχούσες* ακέραιες περιοχές (με το επίθετο *ελάχιστο* υπενθυμίζον απλώς την *προέλευση* τού όρου) χρησιμοποιείται μια ελαφρά παραλλαγή τής ανωτέρω προτάσεως 5.1.5 (βλ.

[1] Η *ελαφρά παραλλαγή* έγκειται στο ότι ο (γενικευμένος) μέγιστος κοινός διαιρέτης (όταν υπάρχει), δεν υποχρεούται να ανήκει κατ' ανάγκην σε κάποιο *προκαθορισμένο* γνήσιο υποσύνολο τής ακεραίας περιοχής αναφοράς.

ορισμό 5.2.20). Βεβαίως, *και εδώ* δεν πρέπει να θεωρείται εν γένει ως δεδομένη *ούτε η ύπαρξη* (τέτοιων γενικευμένων) ελαχίστων κοινών πολλαπλασίων *ούτε η μοναδικότητά τους* (όταν υπάρχουν).

► **Ο ρόλος των πρώτων αριθμών**. Οι *πρώτοι αριθμοί* (ήτοι οι ακέραιοι αριθμοί $p \geq 2$ οι έχοντες τους ± 1 και $\pm p$ ως μοναδικούς διαιρέτες τους) αποτελούν τους *δομικούς λίθους* των μη μηδενικών ακεραίων αριθμών υπό την εξής έννοια: Κάθε $a \in \mathbb{Z} \setminus \{0, \pm 1\}$ παριστάται ως γινόμενο

$$\boxed{a = \text{sign}(a) p_1^{\nu_1} p_2^{\nu_2} \cdots p_k^{\nu_k},} \tag{5.2}$$

όπου $k \in \mathbb{N}$ και $p_1, \ldots, p_k$ κατάλληλοι σαφώς διακεκριμένοι πρώτοι αριθμοί υψούμενοι σε κατάλληλες θετικές ακέραιες δυνάμεις $\nu_1, \ldots, \nu_k$. (Η παράσταση αυτή είναι *μονοσημάντως ορισμένη*, μη λαμβανομένης υπ' όψιν τής διατάξεως των $p_1, \ldots, p_k$, για κάθε $a \in \mathbb{Z} \setminus \{0, \pm 1\}$.) Δύο ικανές και αναγκαίες συνθήκες, υπό τις οποίες η απόλυτη τιμή ενός ακεραίου αριθμού είναι πρώτος αριθμός, δίδονται στις προτάσεις 5.1.7 και 5.1.8.

5.1.7 Πρόταση. *Έστω $n \in \mathbb{Z}$. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Ο $|n|$ είναι πρώτος αριθμός.*

(ii) *$n \in \mathbb{Z} \setminus \{0, \pm 1\}$ και για $a, b \in \mathbb{Z}$ ισχύει η συνεπαγωγή*:

$$[n \mid ab \Longrightarrow \text{είτε } n \mid a \text{ είτε } n \mid b].$$

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Επειδή ο $|n|$ είναι πρώτος αριθμός, έχουμε $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. Επιπροσθέτως, εάν $a, b \in \mathbb{Z}$ και $n \mid ab$, τότε υπάρχει κάποιος $k \in \mathbb{Z} : ab = nk$. Στην περίπτωση όπου $ab = 0$, έχουμε είτε $a = 0$ είτε $b = 0$, οπότε $k = 0$ και είτε $n \mid a$ είτε $n \mid b$. Προφανώς, $ab \notin \{\pm 1\}$ (διότι $k \in \mathbb{Z} \setminus \{0\}$ και $|n| \geq 2$). Στην περίπτωση όπου $|ab| \geq 2$, ο $|n|$, όντας πρώτος αριθμός, είναι διαιρέτης τουλάχιστον ενός εκ των $|a|, |b|$, οπότε είτε $n \mid a$ είτε $n \mid b$.

(ii)⇒(i) Εάν $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ και εάν θεωρήσουμε τυχόντα $a \in \mathbb{Z} \setminus \{0\}$ που είναι διαιρέτης τού n, τότε υπάρχει κάποιος $b \in \mathbb{Z} \setminus \{0\} : n = ab$. Επειδή $ab = n \cdot 1$, έχουμε $n \mid ab$, οπότε (εξ υποθέσεως) είτε $n \mid a$ είτε $n \mid b$. Εάν $n \mid a$, τότε $|n| = |a|$ και $|b| = 1$, οπότε ο $|n|$ είναι πρώτος αριθμός. Κατ' αναλογίαν, εάν $n \mid b$, τότε $|n| = |b|$ και $|a| = 1$, οπότε ο $|n|$ είναι πρώτος αριθμός. □

5.1.8 Πρόταση. *Έστω $n \in \mathbb{Z}$. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Ο $|n|$ είναι πρώτος αριθμός.*

(ii) *$n \in \mathbb{Z} \setminus \{0, \pm 1\}$ και για $a, b \in \mathbb{Z}$ ισχύει η συνεπαγωγή*:

$$[n = ab \Longrightarrow \text{είτε } a \in \{\pm 1\} \text{ είτε } b \in \{\pm 1\}].$$

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Επειδή ο $|n|$ είναι πρώτος αριθμός, έχουμε $n \in \mathbb{Z}\setminus\{0, \pm 1\}$. Επιπροσθέτως, εάν $a, b \in \mathbb{Z}$ και $n = ab$, τότε $|n| = |a|\,|b|$, οπότε *είτε* $|n| = |a|$ και $|b| = 1$ ($\Leftrightarrow b \in \{\pm 1\}$) *είτε* $|n| = |b|$ και $|a| = 1$ ($\Leftrightarrow a \in \{\pm 1\}$).
(ii)⇒(i) Εάν $n \in \mathbb{Z}\setminus\{0, \pm 1\}$ και εάν θεωρήσουμε τυχόντα $a \in \mathbb{Z}\setminus\{0\}$ που διαιρεί τον n, τότε υπάρχει κάποιος $b \in \mathbb{Z}\setminus\{0\} : n = ab$. Εξ υποθέσεως, είτε $a \in \{\pm 1\}$ είτε $b \in \{\pm 1\}$. Εάν $a \in \{\pm 1\}$, τότε $|n| = |b|$ και εάν $b \in \{\pm 1\}$, τότε $|n| = |a|$, οπότε το 1 και ο $|n|$ είναι οι μόνοι θετικοί διαιρέτες τού $|n|$. Αυτό σημαίνει ότι ο $|n|$ είναι πρώτος αριθμός. □

5.1.9 Σημείωση. Για τη γενίκευση τής εννοίας τού πρώτου αριθμού σε *τυχούσες* ακέραιες περιοχές χρησιμοποιούνται *άμεσες* γενικεύσεις αμφοτέρων των συνθηκών 5.1.7 (ii) και 5.1.8 (ii). Αυτές οδηγούν στους ορισμούς των εννοιών *πρώτο στοιχείο* και *ανάγωγο στοιχείο* (βλ. 5.3.1 και 5.3.2, αντιστοίχως). Παρότι οι συνθήκες 5.1.7 (ii) και 5.1.8 (ii) είναι ισοδύναμες στον $\mathbb{Z}$, ένα ανάγωγο στοιχείο μιας ακεραίας περιοχής που δεν είναι Π.Κ.Ι. (ή τουλάχιστον Π.Μ.Π.) δεν είναι κατ' ανάγκην πρώτο! (Βλ. 5.3.3 (iv), 5.3.4 (iii), (iv), και 5.6.3 (ii).)

Δοθέντων n μη μηδενικών ακεραίων αριθμών $a_1, \ldots, a_n$ $(n \in \mathbb{N},\ n \geq 2)$, είναι δυνατόν να δοθούν χρήσιμες εκφράσεις για τον μκδ$(a_1, \ldots, a_n)$ και το εκπ$(a_1, \ldots, a_n)$ μέσω τής παραστάσεως (5.2) καθενός εξ αυτών ως γινομένου πρώτων αριθμών.

5.1.10 Πρόταση. *Εάν* $n \in \mathbb{N},\ n \geq 2$, *και* $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$ *με*

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

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

$$\boxed{\text{μκδ}(a_1, \ldots, a_n) = \prod_{l=1}^{k} p_l^{\min\{\nu_{1,l}, \ldots, \nu_{n,l}\}}} \tag{5.3}$$

και

$$\boxed{\text{εκπ}(a_1, \ldots, a_n) = \prod_{l=1}^{k} p_l^{\max\{\nu_{1,l}, \ldots, \nu_{n,l}\}}.} \tag{5.4}$$

Τέλος, ο μέγιστος κοινός διαιρέτης και το ελάχιστο κοινό πολλαπλάσιο δύο ακεραίων αριθμών συσχετίζονται ως ακολούθως:

5.1.11 Πρόταση. *Για οιουσδήποτε* $a, b \in \mathbb{Z}$ *έχουμε*

$$\boxed{\text{μκδ}(a, b)\text{εκπ}(a, b) = |ab|\,.} \tag{5.5}$$

5.1.12 Σημείωση. Κατάλληλες γενικεύσεις των (5.3), (5.4) και (5.5) εξακολουθούν να ισχύουν στις λεγόμενες *περιοχές μονοσήμαντης παραγοντοποιήσεως*. (Βλ. ορισμό 5.6.2, θεώρημα 5.6.13 και πόρισμα 5.6.14.)

5.2 ΘΕΜΕΛΙΩΔΕΙΣ ΟΡΙΣΜΟΙ ΚΑΙ ΙΔΙΟΤΗΤΕΣ

5.2.1 Ορισμός. Έστω R ένας μεταθετικός δακτύλιος.

(i) Έστω $a \in R$. Λέμε ότι το a είναι **διαιρέτης** ενός $b \in R$ (*εντός τού* R και σημειώνουμε[2]: $a \mid b$) όταν υπάρχει κάποιο στοιχείο $x \in R$, τέτοιο ώστε να ισχύει η ισότητα $b = ax$.

(ii) Δυο στοιχεία $a, b \in R$ λέγονται **συντροφικά** (ή **συνεταιρικά**) όταν $a \mid b$ και, ταυτοχρόνως, $b \mid a$. Επίσης, όταν ικανοποιούνται αυτές οι συνθήκες, αναφέρουμε το a ως **σύντροφο** τού b (ή, ισοδυνάμως, λόγω συμμετρίας, το b ως σύντροφο τού a).

5.2.2 Παραδείγματα. (i) Εντός τού δακτυλίου $\mathbb{Z}[i]$ των ακεραίων τού Gauss το στοιχείο $3 - 4i$ είναι διαιρέτης τού $89 - 77i$, διότι

$$(3 - 4i)\,(23 + 5i) = 89 - 77i.$$

(ii) Εντός τού δακτυλίου $\mathbb{R} \times \mathbb{Z}$ τού καρτεσιανού γινομένου τού σώματος $\mathbb{R}$ των πραγματικών αριθμών και τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών (βλ. 1.1.4 (v)) ισχύουν οι ισότητες

$$(\sqrt{11}\pi^2, 7)(\sqrt{11}\pi^{-2}, 1) = (11, 7)\,, \quad (11, 7)\,(11^{-\frac{1}{2}}\pi^2, 1) = (\sqrt{11}\pi^2, 7),$$

(όπου[3] $\pi = 3,14159...$), οπότε τα στοιχεία $(\sqrt{11}\pi^2, 7)$ και $(11, 7)$ είναι συντροφικά.

5.2.3 Πρόταση. *Έστω R ένας μεταθετικός δακτύλιος. Τότε ισχύουν τα ακόλουθα*:

(i) $a \mid 0_R,\ \forall a \in R$, *και εάν* $b \in R$ *και* $0_R \mid b$, *τότε* $b = 0_R$.

(ii) *Εάν* $a,\ b \in R$ *και* $a \mid b$, *τότε* $ac \mid bc,\ \ \forall c \in R$.

(iii) *Εάν* $a, b, c \in R$, *τέτοια ώστε* $a \mid b$ *και* $b \mid c$, *τότε* $a \mid c$.

(iv) *Εάν* $a, b, c \in R$, *τέτοια ώστε* $a \mid b$ *και* $a \mid c$, *τότε*[4]

$$a \mid bx + cy, \quad \forall\,(x, y)\ \in R \times R.$$

(v) *Εάν ο R δεν είναι τετριμμένος δακτύλιος και έχει μοναδιαίο στοιχείο, τότε* $a \mid a$, $1_R \mid a,\ \forall a \in R$ *και*

$$a \mid 1_R \iff a \in R^{\times}.$$

[2] Κατ' αναλογίαν, όταν το a δεν διαιρεί το b, γράφουμε $a \nmid b$.

[3] $\pi =$ ο λόγος τού μήκους τής περιφέρειας ενός κύκλου προς τη διάμετρό του.

[4] Γενικότερα, εάν $n \in \mathbb{N}$, $b_1, \ldots, b_n \in R$, 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 οιαδήποτε $x_1, \ldots, x_n \in R$.

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $0_R = 0_R \cdot a$, οπότε $a \mid 0_R$ για κάθε $a \in R$. Και εάν $b \in R$ και $0_R \mid b$, τότε $\exists c \in R : b = c \cdot 0_R = 0_R$.

(ii) Για κάθε $c \in R$ έχουμε

$$a \mid b \Longrightarrow (\exists x \in R : b = ax) \Longrightarrow (\exists x \in R : bc = acx) \Longrightarrow ac \mid bc.$$

(iii) Εάν $a, b, c \in R$, με $a \mid b$ και $b \mid c$, τότε υπάρχουν $x, y \in R$, τέτοια ώστε

$$\left.\begin{array}{c} b = ax \\ c = by \end{array}\right\} \Longrightarrow c = axy \Longrightarrow a \mid c.$$

(iv) Εάν $a, b, c \in R$, με $a \mid b$ και $a \mid c$, τότε υπάρχουν $a', a'' \in R$, τέτοια ώστε για οιαδήποτε $x, y \in R$ να ισχύει

$$\left.\begin{array}{c} b = aa' \\ c = aa'' \end{array}\right\} \Longrightarrow bx + cy = a\,(a'x + a''y) \Longrightarrow a \mid bx + cy.$$

(v) Προφανώς, $a = a \cdot 1_R = 1_R \cdot a$ για κάθε $a \in R$ και

$$a \mid 1_R \Longleftrightarrow \exists x \in R : 1_R = ax,$$

το οποίο, λόγω τής ιδιότητας τής μεταθετικότητας εντός τού R ($ax = xa$) ισοδυναμεί με το ότι $a \in R^\times$. □

5.2.4 Πρόταση. *Έστω R ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν $a, b, u \in R$, τότε ισχύουν τα ακόλουθα*:

(i) $a \mid b \Longleftrightarrow \langle b\rangle \subseteq \langle a\rangle$.

(ii) *Τα a και b είναι συντροφικά* $\Longleftrightarrow \langle a\rangle = \langle b\rangle$.

(iii) *Η σχέση* $[a \underset{\text{συν.}}{\sim} b \underset{\text{ορσ}}{\Longleftrightarrow}$ *τα a και b είναι συντροφικά* $]$ *αποτελεί μια σχέση ισοδυναμίας επί τού R.*

(iv) $u \underset{\text{συν.}}{\sim} 0_R \Longleftrightarrow u = 0_R$, $u \underset{\text{συν.}}{\sim} 1_R \Longleftrightarrow u \in R^\times$ *και*

$$u \in R^\times \Longleftrightarrow u \mid r, \quad \forall r \in R$$

(v) *Εάν $a = bx$, όπου $x \in R^\times$, τότε τα a και b είναι συντροφικά. Εάν, μάλιστα, ο R είναι ακεραία περιοχή, τότε ισχύει και το αντίστροφο.*

ΑΠΟΔΕΙΞΗ. (i) Εάν $a \mid b$, τότε υπάρχει κάποιο $x \in R$ με $b = ax$, οπότε $b \in \langle a\rangle$. Εξάλλου, για οιοδήποτε $c \in \langle b\rangle$ υπάρχει κάποιο y με $c = by$, οπότε

$$c = (ax)\,y = a(xy) \Longrightarrow c \in \langle a\rangle \Longrightarrow \langle b\rangle \subseteq \langle a\rangle.$$

(ii) Προφανώς, τα a και b είναι συντροφικά εάν και μόνον εάν

$$a \mid b \ \text{ και } \ b \mid a \underset{\text{(i)}}{\Longleftrightarrow} \langle b\rangle \subseteq \langle a\rangle \ \text{ και } \ \langle a\rangle \subseteq \langle b\rangle \Longleftrightarrow \langle a\rangle = \langle b\rangle.$$

(iii) Πρόδηλο λόγω τού (ii).

(iv) Η πρώτη αμφίπλευρη συνεπαγωγή έπεται από το (i) και η δεύτερη από το (v) τής προτάσεως 5.2.3. Σε ό,τι αφορά στην τρίτη, εάν το u είναι αντιστρέψιμο, τότε

$$r = u\left(u^{-1}r\right), \ \ \forall r \in R \Longrightarrow u \mid r, \ \ \forall r \in R.$$

Και αντιστρόφως· εάν $u \mid r$ για κάθε $r \in R$, θέτοντας $r = 1_R$ λαμβάνουμε την αμφίπλευρη συνεπαγωγή $u \mid 1_R \Longleftrightarrow u \in R^\times$ (βλ. το (v) τής προτάσεως 5.2.3).

(v) Εάν $a = bx$, όπου $x \in R^\times$, τότε $b = ax^{-1}$, οπότε $a \underset{\text{συν.}}{\sim} b$. Και αντιστρόφως· εάν ο R είναι ακεραία περιοχή και $a \underset{\text{συν.}}{\sim} b$, τότε υπάρχουν $x, y \in R$, τέτοια ώστε

$$\left.\begin{array}{l} a = bx \\ b = ay \end{array}\right\} \Longrightarrow a = axy,$$

απ' όπου έπεται ότι *είτε* $a = b = 0_R$ (οπότε $0_R = 0_R \cdot u, \ \forall u \in R^\times$) *είτε* $1_R = xy$ (βλ. 1.2.5), ήτοι $x, y \in R^\times$. □

5.2.5 Πόρισμα. *Για κάθε ζεύγος a, b στοιχείων μιας ακεραίας περιοχής R ισχύει η αμφίπλευρη συνεπαγωγή* :

$$\boxed{a \underset{\text{συν.}}{\sim} b \Longleftrightarrow \left[\exists x \in R^\times : a = bx\right].}$$

(Αυτό το x είναι μονοσημάντως ορισμένο *όταν $a, b \in R \setminus \{0_R\}$.)*

ΑΠΟΔΕΙΞΗ. Η ανωτέρω αμφίπλευρη συνεπαγωγή είναι αληθής λόγω τού (v) τής προτάσεως 5.2.4. Όταν τα a, b είναι μη μηδενικά, αυτό το $x \in R^\times$ είναι μονοσημάντως ορισμένο λόγω τού κανόνα τής διαγραφής 1.2.5. □

5.2.6 Παραδείγματα. (i) Εντός ενός σώματος K *οιαδήποτε* στοιχεία a, b τού $K \setminus \{0_K\}$ είναι συντροφικά, διότι $a = bb^{-1}a$ και $b^{-1}a \in K^\times = K \setminus \{0_K\}$.

(ii) Εντός τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών τα μόνα συντροφικά στοιχεία ενός $n \in \mathbb{Z}$ είναι τα $\pm n$, καθότι $\mathbb{Z}^\times = \{\pm 1\}$.

5.2.7 Παρατήρηση. Έστω R μια ακεραία περιοχή. Εάν τα a, b, c, d είναι στοιχεία τής R με $a \underset{\text{συν.}}{\sim} b$ και $c \underset{\text{συν.}}{\sim} d$, τότε $ac \underset{\text{συν.}}{\sim} bd$. (Πράγματι· εάν υπάρχουν $x, y \in R^\times$, τέτοια να ισχύουν οι ισότητες $a = bx$ και $c = dy$, τότε $ac = bd(xy)$, όπου $xy \in R^\times$.) Ωστόσο, εν γένει *δεν* ισχύει $a + c \underset{\text{συν.}}{\sim} b + d$, όπως διαπιστώνουμε, επί παραδείγματι, όταν $R = \mathbb{Z}[i]$, $a = b = 1$ και $c = 1 + 2i$, $d = -2 + i$. (Πράγματι· $1 \underset{\text{συν.}}{\sim} 1$ και $1 + 2i = i\,(-2 + i)$, οπότε $1 + 2i \underset{\text{συν.}}{\sim} -2 + i$, αλλά τα $2 + 2i$ και $-1 + i$ δεν είναι συντροφικά.)

5.2.8 Σημείωση. Έστω b ένα στοιχείο μιας ακεραίας περιοχής R. Επειδή οι σύντροφοι τού b και τα αντιστρέψιμα στοιχεία τής R είναι *πάντοτε* διαιρέτες τού b, είθισται κάθε $a \in R \setminus R^\times$, το οποίο είναι διαιρέτης τού b χωρίς να είναι ταυτοχρόνως και σύντροφός του, να καλείται **γνήσιος διαιρέτης** τού b. (Προφανώς, σύμφωνα με αυτόν τον ορισμό, τα αντιστρέψιμα στοιχεία τής R δεν διαθέτουν κανέναν γνήσιο διαιρέτη, ενώ οι γνήσιοι διαιρέτες τού 0_R είναι τα στοιχεία τού συνόλου $R \setminus (R^\times \cup \{0_R\})$.)

(i) Βάσει τού (i) τής προτάσεως 5.2.4, *το a είναι γνήσιος διαιρέτης τού b εάν και μόνον εάν* $\langle b\rangle \subsetneqq \langle a\rangle \subsetneqq R$.

(ii) Εάν $a, b \in R, c \in R\setminus\{0_R\}$ και $c = ab$, τότε *το στοιχείο a είναι γνήσιος διαιρέτης τού c* $\iff$ *το b είναι γνήσιος διαιρέτης τού c.* (Τούτο έπεται άμεσα από τις αμφίπλευρες συνεπαγωγές $b \in R^\times \iff a \underset{\text{συν.}}{\sim} c$ και $a \in R^\times \iff b \underset{\text{συν.}}{\sim} c$.)

5.2.9 Ορισμός. Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N},\ n \geq 2$, και τα $a_1, \ldots, a_n$ στοιχεία τού R, τότε ένα στοιχείο $d \in R$ καλείται **μέγιστος κοινός διαιρέτης** των $a_1, \ldots, a_n$ όταν ισχύουν τα ακόλουθα:

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

(ii) για οιοδήποτε $c \in R$, για το οποίο ισχύει $c \mid a_1, \ldots, c \mid a_n$, έχουμε $c \mid d$.

Θέτουμε

$$\boxed{\text{ΜΚΔ}_R(a_1, \ldots, a_n) := \left\{ d \in R \,\middle|\, \begin{array}{c} d \text{ μέγιστος κοινός} \\ \text{διαιρέτης των } a_1, \ldots, a_n \end{array} \right\}.}$$

5.2.10 Παραδείγματα. (i) Εάν $a_1, \ldots, a_n \in \mathbb{Z}$, τότε (κάνοντας χρήση τού συνήθους ορισμού τού μκδ$(a_1, \ldots, a_n)$ τού θεσπιζόμενου εντός τού πλαισίου τής Στοιχειώδους Θεωρίας Αριθμών) διαπιστώνουμε ότι

$$\text{ΜΚΔ}_{\mathbb{Z}}(a_1, \ldots, a_n) = \{\pm\text{μκδ}(a_1, \ldots, a_n)\}.$$

Κατά συνέπειαν, στον $\mathbb{Z}$, από *δακτυλιοθεωρητική σκοπιά* (ήτοι ακολουθώντας τον ορισμό 5.2.9), οι $a_1, \ldots, a_n$ έχουν *αμφότερους* τους μκδ$(a_1, \ldots, a_n)$ και $-$μκδ$(a_1, \ldots, a_n)$ ως μεγίστους κοινούς διαιρέτες τους και

$$\text{μκδ}(a_1, \ldots, a_n) \neq -\text{μκδ}(a_1, \ldots, a_n) \Leftrightarrow \exists j \in \{1, \ldots, n\} : a_j \neq 0.$$

(ii) Θεωρούμε το σύνολο $M = \{1, 2, 3, 4, 5, 6\}$ και το δυναμοσύνολό του $\mathfrak{P}(M)$. Σύμφωνα με την άσκηση **1-9**, η τριάδα $(\mathfrak{P}(M), \triangle, \cap)$ αποτελεί έναν μεταθετικό δακτύλιο με μοναδιαίο στοιχείο. Εάν

$$A_1 = \{2\},\ A_2 = \{2, 3\},\ A_3 = \{1, 3\},\ B = \{1, 2, 3\},$$

τότε

$$A_1 \cap B = A_1,\ \ A_2 \cap B = A_2,\ \ A_3 \cap B = A_3 \Longrightarrow B \mid A_j,\ j = 1, 2, 3.$$

Εξάλλου, οιοδήποτε στοιχείο $C \in \mathfrak{P}(M)$ είναι διαιρέτης των A_j, $j = 1, 2, 3$, οφείλει να περιέχει το B, οπότε

$$B \subseteq C \Longrightarrow B = C \cap B \Longrightarrow C \mid B.$$

Επομένως, $B \in \text{ΜΚΔ}_{\mathfrak{P}(M)}(A_1, A_2, A_3)$.

5.2.11 Σημείωση. Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N}$, $n \geq 2$, και τα $a_1, \ldots, a_n$ στοιχεία τού R, τότε

(i) το σύνολο $\text{ΜΚΔ}_R(a_1, \ldots, a_n)$ δεν είναι κατ' ανάγκην μη κενό (βλ. 5.2.43 (i)),

(ii) το $\text{ΜΚΔ}_R(a_1, \ldots, a_n)$ δεν είναι κατ' ανάγκην μονοσύνολο (βλ. 5.2.10 (i)) και

(iii) όταν $\text{ΜΚΔ}_R(a_1, \ldots, a_n) \neq \varnothing$, κάθε μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$ είναι *μονοσημάντως ορισμένος μέχρις συντροφικότητας* (ήτοι οιοσδήποτε άλλος μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$ οφείλει να είναι σύντροφος αυτού). Τούτο αποδεικνύεται στην επόμενη πρόταση.

5.2.12 Πρόταση. *Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N}$, $n \geq 2$, τα $a_1, \ldots, a_n$ στοιχεία τού R και $d \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$, τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $d \underset{\text{συν.}}{\sim} d'$, για κάποιο $d' \in R$, τότε $d' \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$.*

(ii) *Εάν $d' \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$, τότε $d \underset{\text{συν.}}{\sim} d'$.*

ΑΠΟΔΕΙΞΗ. (i) Εάν $d \underset{\text{συν.}}{\sim} d'$, για κάποιο $d' \in R$, τότε

$$\left.\begin{array}{r} d' \mid d \Longrightarrow \exists x \in R : d = d'x \\ \exists a'_j \in R : a_j = da'_j,\ \forall j \in \{1, ..., n\} \end{array}\right\} \Longrightarrow a_j = d'xa'_j,\ \forall j \in \{1, ..., n\},$$

οπότε $d' \mid a_j$ για κάθε $j \in \{1, ..., n\}$. Εξάλλου, για οιοδήποτε $c \in R$, για το οποίο ισχύει $c \mid a_1, \ldots, c \mid a_n$, έχουμε $c \mid d$ και κατ' επέκταση $c \mid d'$ (αφού εξ υποθέσεως $d \mid d'$, βλ. 5.2.3 (iii)).

(ii) Εάν το $d' \in R$ είναι ένας μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$, τότε λόγω των (i) και (ii) τού ορισμού 5.2.9 ισχύουν οι σχέσεις διαιρετότητας $d \mid d'$ και $d' \mid d$, οπότε $d \underset{\text{συν.}}{\sim} d'$. □

5.2.13 Πόρισμα. *Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N}$, $n \geq 2$, τα $a_1, \ldots, a_n$ στοιχεία τού R και $d \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$, τότε*

$$d = 0_R \Longleftrightarrow a_1 = \cdots = a_n = 0_R \Longleftrightarrow \text{ΜΚΔ}_R(a_1, \ldots, a_n) = \{0_R\}.$$

Κατά συνέπειαν,

$$d \in R \setminus \{0_R\} \Longleftrightarrow \exists j \in \{1, \ldots, n\} : a_j \in R \setminus \{0_R\}.$$

ΑΠΟΔΕΙΞΗ. Εάν $d = 0_R$, τότε $0_R \mid a_j$ για κάθε $j \in \{1, \dots, n\}$, οπότε λόγω τού (i) τής προτάσεως 5.2.3 λαμβάνουμε $a_1 = \cdots = a_n = 0_R$. Και αντιστρόφως· εάν ισχύει $a_1 = \cdots = a_n = 0_R$, τότε το 0_R πληροί αμφότερες τις συνθήκες (i) και (ii) τού ορισμού 5.2.9, οπότε $0_R \in \text{ΜΚΔ}_R(0_R, \dots, 0_R)$. Έστω τυχών $d \in \text{ΜΚΔ}_R(0_R, \dots, 0_R)$. Τότε $d \underset{\text{συν.}}{\sim} 0_R$ (λόγω τού (ii) τής προτάσεως 5.2.12), οπότε $d = 0_R$ (λόγω τού (iv) τής προτάσεως 5.2.4). □

5.2.14 Θεώρημα. *Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $d, a_1, a_2, \dots, a_n$ είναι στοιχεία ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο, τότε τα ακόλουθα είναι ισοδύναμα*:

(i) $d \in \text{ΜΚΔ}_R(a_1, \dots, a_n)$ *και*

$$d = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$$

για κάποια $r_1, r_2, \dots, r_n \in R$.

(ii) $\langle d \rangle = \langle a_1, a_2, \dots, a_n \rangle \ \left(= \langle a_1 \rangle + \langle a_2 \rangle \cdots + \langle a_n \rangle\right)$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν το d είναι ένας μέγιστος κοινός διαιρέτης των $a_1, \dots, a_n$ και $d = r_1 a_1 + \cdots + r_n a_n$ για κάποια $r_1, \dots, r_n \in R$, τότε προφανώς

$$d \in \langle a_1, a_2, \dots, a_n \rangle \Longrightarrow \langle d \rangle \subseteq \langle a_1, a_2, \dots, a_n \rangle .$$

Εξάλλου, για κάθε $j \in \{1, \dots, n\}$ έχουμε $d \mid a_j \Longrightarrow (\exists x_j \in R : a_j = x_j d)$, οπότε για οιοδήποτε στοιχείο

$$s_1 a_1 + s_2 a_2 + \cdots + s_n a_n \in \langle a_1, a_2, \dots, a_n \rangle , \ \ s_1, \dots, s_n \in R,$$

διαπιστώνουμε ότι

$$s_1 a_1 + \cdots + s_n a_n = (s_1 x_1 + \cdots + s_n x_n)\, d \in \langle d \rangle .$$

Άρα τελικώς $\langle d \rangle = \langle a_1, a_2, \dots, a_n \rangle$.

(ii)⇒(i) Εάν $\langle d \rangle = \langle a_1, a_2, \dots, a_n \rangle$, τότε προφανώς $d = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$ για κάποια $r_1, r_2, \dots, r_n \in R$. Επιπροσθέτως, για κάθε $j \in \{1, \dots, n\}$ έχουμε

$$a_j \in \langle d \rangle \Longrightarrow d \mid a_j .$$

Εξάλλου, οιοδήποτε $c \in R$, για το οποίο ισχύει $c \mid a_1, \dots, c \mid a_n$, είναι διαιρέτης τού $d = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$ (βλ. 5.2.3 (v)). Άρα το d είναι ένας μέγιστος κοινός διαιρέτης των $a_1, a_2, \dots, a_n$. □

5.2.15 Πόρισμα. *Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $a_1, a_2, \dots, a_n$ είναι στοιχεία ενός μεταθετικού δακτυλίου κυρίων ιδεωδών R με μοναδιαίο στοιχείο, τότε*

$\text{ΜΚΔ}_R(a_1, \dots, a_n) \neq \varnothing$, *ενώ κάθε* $d \in \text{ΜΚΔ}_R(a_1, \dots, a_n)$ *παριστάται υπό τη μορφή*

$$\boxed{d = r_1a_1 + r_2a_2 + \cdots + r_na_n,} \tag{5.6}$$

για κάποια $r_1, r_2, \dots, r_n \in R$.

ΑΠΟΔΕΙΞΗ. Επειδή ο R είναι Δ.Κ.Ι., υπάρχει κάποιο στοιχείο $d' \in R$, τέτοιο ώστε να ισχύει η ισότητα $\langle d' \rangle = \langle a_1, a_2, \dots, a_n \rangle$, οπότε το d' γράφεται υπό τη μορφή (5.6). Κατά το θεώρημα 5.2.14 το d' είναι ένας μέγιστος κοινός διαιρέτης των $a_1, a_2, \dots, a_n$. Αλλά και *οιοσδήποτε* μέγιστος κοινός διαιρέτης d των $a_1, a_2, \dots, a_n$ μπορεί να γραφεί κατ' αυτόν τον τρόπο, αφού $d \underset{\text{συν.}}{\sim} d'$, πράγμα που σημαίνει ότι $\langle d \rangle = \langle d' \rangle$. □

5.2.16 Ορισμός. Έστω ότι $n \in \mathbb{N}$, $n \geq 2$, και ότι τα $a_1, a_2, \dots, a_n$ είναι μη μηδενικά στοιχεία ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο. Λέμε ότι τα $a_1, a_2, \dots, a_n$ είναι **σχετικώς πρώτα** (ή ότι είναι **μεταξύ τους πρώτα**) όταν

$$1_R \in \text{ΜΚΔ}_R(a_1, \dots, a_n).$$

5.2.17 Πόρισμα. (Bézout) *Εάν* $n \in \mathbb{N}$, $n \geq 2$, *και εάν τα* $a_1, a_2, \dots, a_n$ *είναι στοιχεία ενός μεταθετικού δακτυλίου κυρίων ιδεωδών* R *με μοναδιαίο στοιχείο, τότε τα* $a_1, a_2, \dots, a_n$ *είναι σχετικώς πρώτα εάν και μόνον εάν*

$$r_1a_1 + r_2a_2 + \cdots + r_na_n = 1_R, \tag{5.7}$$

για κάποια $r_1, r_2, \dots, r_n \in R$, *ή -ισοδυνάμως- εάν και μόνον εάν*

$$Ra_1 + Ra_2 + \cdots + Ra_n = R.$$

ΑΠΟΔΕΙΞΗ. Εάν τα $a_1, a_2, \dots, a_n$ είναι σχετικώς πρώτα, τότε ένας μέγιστος κοινός διαιρέτης τους είναι το 1_R, οπότε ο ισχυρισμός είναι αληθής επί τη βάσει τού πορίσματος 5.2.15. Και αντιστρόφως· εάν

$$r_1a_1 + r_2a_2 + \cdots + r_na_n = 1_R,$$

για κάποια $r_1, r_2, \dots, r_n \in R$, τότε για οιοδήποτε στοιχείο $c \in R$, για το οποίο ισχύει $c \mid a_1, \dots, c \mid a_n$, έχουμε $c \mid 1_R$ (βλ. το (iv) τής προτάσεως 5.2.3). Επειδή προφανώς $1_R \mid a_1, \dots, 1_R \mid a_n$, συμπεραίνουμε (απευθείας απο τον ορισμό 5.2.9) ότι $1_R \in \text{ΜΚΔ}_R(a_1, \dots, a_n)$. □

5.2.18 Σημείωση. Εάν ο R δεν είναι Δ.Κ.Ι., τότε οι ισότητες (5.6) και (5.7) δεν ισχύουν πάντοτε. Όταν, π.χ., $R = \mathbb{Z}[\sqrt{-5}]$, τότε τα 2 και $1 + \sqrt{-5}$ είναι σχετικώς πρώτα, χωρίς να υφίσταται ισότητα τής μορφής (5.7). Πράγματι· το 1 είναι

(προφανής) διαιρέτης αυτών των στοιχείων. Υποθέτοντας ότι υπάρχουν κάποιοι $a, b \in \mathbb{Z}$ (με τουλάχιστον έναν εξ αυτών διάφορο τού μηδενός), τέτοιοι ώστε

$$a + b\sqrt{-5} \mid 2, \quad a + b\sqrt{-5} \mid 1 + \sqrt{-5},$$

θα υπάρχουν κάποιοι $x, y \in \mathbb{Z}$ με

$$1 + \sqrt{-5} = (x + y\sqrt{-5})(a + b\sqrt{-5}) = (ax - 5y) + (bx + ay)\sqrt{-5},$$

Κατά συνέπειαν,

$$\left\{ \begin{array}{l} ax - 5y = 1, \\ bx + ay = 1 \end{array} \right\} \Longrightarrow \left\{ \begin{array}{l} x = \frac{a+5b}{a^2+5b^2}, \\ y = \frac{a-b}{a^2+5b^2} \end{array} \right\}. \tag{5.8}$$

Διακρίνουμε τρεις περιπτώσεις: (i) $a = b$. Τότε $x = \frac{1}{a}$, και επειδή $x \in \mathbb{Z}$ έχουμε $a = \pm 1$, οπότε

$$a + b\sqrt{-5} = \pm\left(1 + \sqrt{-5}\right).$$

Επειδή αυτό είναι διαιρέτης *και* τού 2, θα πρέπει να ισχύει η ισότητα

$$2 = (1 + \sqrt{-5})(\mu + \nu\sqrt{-5}), \tag{5.9}$$

για κάποιους $\mu, \nu \in \mathbb{Z}$. Θεωρώντας τούς συζυγείς και στα δύο μέλη τής (5.9) καταλήγουμε στην

$$2 = (1 - \sqrt{-5})(\mu - \nu\sqrt{-5}). \tag{5.10}$$

Πολλαπλασιάζοντας κατά μέλη τις (5.9) και (5.10) λαμβάνουμε

$$4 = 6\left(\mu^2 + 5\nu^2\right). \tag{5.11}$$

Όμως η ισχύς τής ως άνω ισότητας (5.11) είναι *αδύνατη*, καθότι το δεξιό της μέλος είναι προφανώς > 4, όταν τουλάχιστον ένα εκ των μ, ν είναι διάφορο τού μηδενός, και είναι $= 0$, όταν $\mu = \nu = 0$.

(ii) $a \neq b$ και $b \neq 0$. Σε αυτήν την περίπτωση,

$$1 \leq |a - b| \leq |a| + |b| \leq a^2 + b^2 < a^2 + 5b^2 \Longrightarrow 0 < |y| = \frac{|a - b|}{a^2 + 5b^2} < 1,$$

(βλ. (5.8)), πράγμα *άτοπο*, διότι -εξ υποθέσεως- $y \in \mathbb{Z}$.

(iii) $a \neq b$ και $b = 0$. Στην τελευταία αυτή περίπτωση έχουμε (λόγω των (5.8)):

$$\mathbb{Z} \ni x = y = \frac{1}{a} \Longrightarrow a = \pm 1 \Longrightarrow a + b\sqrt{-5} = \pm 1,$$

που είναι διαιρέτης τού 1. Άρα οι 2 και $1 + \sqrt{-5}$ είναι όντως *σχετικώς πρώτοι*.

Εν συνεχεία, υποθέτοντας ότι υπάρχουν $r_1, r_2 \in \mathbb{Z}[\sqrt{-5}]$, τέτοιοι ώστε να ισχύει η (5.7):

$$2r_1 + \left(1 + \sqrt{-5}\right) r_2 = 1$$

για τα εν λόγω στοιχεία, καταλήγουμε σε *άτοπο*, διότι αυτή ισοδυναμεί με την

$$(1 - \sqrt{-5})(1 + \sqrt{-5})r_1 + 3(1 + \sqrt{-5})r_2 = 3,$$

έχουσα το $1 + \sqrt{-5}$ ως διαιρέτη τού αριστερού της αλλά όχι και τού δεξιού της μέλους! (Στο εδάφιο 4.2.13 είχαμε αποδείξει με ανάλογους συλλογισμούς ότι το ιδεώδες $\langle 2, 1 + \sqrt{-5} \rangle$ δεν είναι κύριο!)

5.2.19 Πρόταση. *Έστω ότι ο R είναι ένας μεταθετικός δακτύλιος κυρίων ιδεωδών με μοναδιαίο στοιχείο και $a, b, c \in R$. Τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $a \mid bc$ και τα a, b είναι σχετικώς πρώτα, τότε $a \mid c$.*

(ii) *Εάν $a \mid c,\ b \mid c$ και τα a, b είναι σχετικώς πρώτα, τότε $ab \mid c$.*

(iii) *Εάν $c \mid a$ και τα a, b είναι σχετικώς πρώτα, τότε και τα c και b είναι σχετικώς πρώτα.*

ΑΠΟΔΕΙΞΗ. Εάν υποθέσουμε ότι τα a, b είναι σχετικώς πρώτα, τότε, σύμφωνα με το πόρισμα 5.2.17, υπάρχουν $u, v \in R$ με $ua + vb = 1_R$.

(i) Εάν $a \mid bc$, τότε

$$\left.\begin{array}{r} c = uac + vbc \\ a \mid uac,\ a \mid vbc \end{array}\right\} \Longrightarrow a \mid c.$$

(ii) Εάν $a \mid c$ και $b \mid c$, τότε

$$\left.\begin{array}{r} c = uac + vbc \\ ab \mid ac,\ ab \mid bc \end{array}\right\} \Longrightarrow ab \mid c.$$

(iii) Εάν $c \mid a$, τότε $\exists x \in R : a = cx$, οπότε

$$\left.\begin{array}{r} ua + vb = 1_R \\ a = cx \end{array}\right\} \Longrightarrow (ux)\, c + vb = 1_R \Longrightarrow 1_R \in \text{ΜΚΔ}_R(c, b).$$

(Εν προκειμένω, έγινε χρήση των (ii) και (iv) τής προτάσεως 5.2.3, και τού πορίσματος 5.2.17, αντιστοίχως.) □

5.2.20 Ορισμός. Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N},\ n \geq 2$, και $a_1, \ldots, a_n \in R$, τότε ένα $t \in R$ καλείται **ελάχιστο κοινό πολλαπλάσιο** των $a_1, \ldots, a_n$ όταν ισχύουν τα ακόλουθα:

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

(ii) για οιοδήποτε $s \in R$, για το οποίο ισχύει $a_1 \mid s, \ldots, a_n \mid s$, έχουμε $t \mid s$.
Θέτουμε

$$\boxed{\text{ΕΚΠ}_R(a_1, \ldots, a_n) := \left\{ t \in R \,\middle|\, \begin{array}{c} t \text{ ελάχιστο κοινό} \\ \text{πολλαπλάσιο των } a_1, \ldots, a_n \end{array} \right\}.}$$

5.2.21 Παραδείγματα. (i) Εάν $a_1, \ldots, a_n \in \mathbb{Z}$, τότε (κάνοντας χρήση τού συνήθους ορισμού τού εκπ$(a_1, \ldots, a_n)$ τού θεσπιζόμενου εντός τού πλαισίου τής Στοιχειώδους Θεωρίας Αριθμών) διαπιστώνουμε ότι

$$\text{ΕΚΠ}_{\mathbb{Z}}(a_1, \ldots, a_n) = \{\pm \text{εκπ}(a_1, \ldots, a_n)\}.$$

Κατά συνέπειαν, στον $\mathbb{Z}$, από *δακτυλιοθεωρητική σκοπιά* (ήτοι ακολουθώντας τον ορισμό 5.2.20), οι $a_1, \ldots, a_n$ έχουν *αμφότερα* τα εκπ$(a_1, \ldots, a_n)$ και $-$εκπ$(a_1, \ldots, a_n)$ ως ελάχιστα κοινά πολλαπλάσιά τους και

$$\text{εκπ}(a_1, \ldots, a_n) \neq -\,\text{εκπ}(a_1, \ldots, a_n) \Leftrightarrow a_j \neq 0,\ \forall j \in \{1, \ldots, n\}.$$

(ii) Θεωρούμε το σύνολο $M = \{1, 2, 3, 4, 5, 6\}$ και το δυναμοσύνολό του $\mathfrak{P}(M)$. Σύμφωνα με την άσκηση **1-9**, η τριάδα $(\mathfrak{P}(M), \triangle, \cap)$ αποτελεί έναν μεταθετικό δακτύλιο με μοναδιαίο στοιχείο. Εάν $B_1 = \{1, 2, 3\}$, $B_2 = \{1, 2, 4\}$, $B_3 = \{1, 2, 3, 4\}$ και $E = \{1, 2\}$, τότε

$$B_1 \cap E = B_2 \cap E = B_3 \cap E = E \Longrightarrow B_j \mid E,\ j = 1, 2, 3.$$

Εξάλλου, οιοδήποτε στοιχείο $C \in \mathfrak{P}(M)$ με τα B_j, $j = 1, 2, 3$, ως διαιρέτες του οφείλει να περιέχεται ταυτοχρόνως στα B_j, $j = 1, 2, 3$, άρα και στην τομή αυτών, οπότε

$$C \subseteq E \Longrightarrow C = C \cap E \Longrightarrow E \mid C.$$

Επομένως, $E \in \text{ΕΚΠ}_{\mathfrak{P}(M)}(B_1, B_2, B_3)$.

5.2.22 Σημείωση. Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N},\ n \geq 2$, και τα $a_1, \ldots, a_n$ στοιχεία τού R, τότε

(i) το σύνολο $\text{ΕΚΠ}_R(a_1, \ldots, a_n)$ δεν είναι κατ' ανάγκην μη κενό (βλ. 5.2.43 (ii)),

(ii) το $\text{ΕΚΠ}_R(a_1, \ldots, a_n)$ δεν είναι κατ' ανάγκην μονοσύνολο (βλ. 5.2.21 (i)) και

(iii) όταν $\text{ΕΚΠ}_R(a_1, \ldots, a_n) \neq \varnothing$, κάθε ελάχιστο κοινό πολλαπλάσιο των $a_1, \ldots, a_n$ είναι *μονοσημάντως ορισμένο μέχρις συντροφικότητας* (ήτοι οιοδήποτε άλλο ελάχιστο κοινό πολλαπλάσιο των $a_1, \ldots, a_n$ οφείλει να είναι σύντροφος αυτού). Τούτο αποδεικνύεται στην επόμενη πρόταση.

5.2.23 Πρόταση. *Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N},\ n \geq 2$, τα $a_1, \ldots, a_n$ στοιχεία τού R και $t \in \text{ΕΚΠ}_R(a_1, \ldots, a_n)$, τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $t \underset{\text{συν.}}{\sim} t'$, για κάποιο $t' \in R$, τότε $t' \in \text{ΕΚΠ}_R(a_1, \ldots, a_n)$.*

(ii) *Εάν το $t' \in \text{ΕΚΠ}_R(a_1, \ldots, a_n)$, τότε $t \underset{\text{συν.}}{\sim} t'$.*

ΑΠΟΔΕΙΞΗ. (i) Εάν $t \underset{\text{συν.}}{\sim} t'$, για κάποιο $t' \in R$, τότε

$$\left.\begin{array}{r} t \mid t' \Longrightarrow \exists x \in R : t' = tx \\ \exists a'_j \in R : t = a_j a'_j,\ \forall j \in \{1, ..., n\} \end{array}\right\} \Longrightarrow t' = a_j a'_j x,\ \forall j \in \{1, ..., n\},$$

οπότε $a_j \mid t'$ για κάθε $j \in \{1, ..., n\}$. Εξάλλου, για οιοδήποτε $s \in R$, για το οποίο ισχύει $a_1 \mid s, \ldots, a_n \mid s$, έχουμε $t \mid s$ και κατ' επέκταση $t' \mid s$ (αφού εξ υποθέσεως $t' \mid t$, βλ. 5.2.3 (iii)).

(ii) Εάν το $t' \in R$ είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, \ldots, a_n$, τότε λόγω των (i) και (ii) τού ορισμού 5.2.20 ισχύουν οι σχέσεις διαιρετότητας $t \mid t'$ και $t' \mid t$, οπότε $t \underset{\text{συν.}}{\sim} t'$. □

5.2.24 Θεώρημα. *Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $t, a_1, a_2, \ldots, a_n$ είναι στοιχεία ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο, τότε τα ακόλουθα είναι ισοδύναμα*:

(i) $t \in \text{ΕΚΠ}_R(a_1, \ldots, a_n)$.

(ii) $\langle t \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_n \rangle$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν το t είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \ldots, a_n$, τότε για κάθε $j \in \{1, \ldots, n\}$ έχουμε $a_j \mid t$, οπότε

$$t \in \langle a_j \rangle \Longrightarrow t \in \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_n \rangle \Longrightarrow \langle t \rangle \subseteq \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_n \rangle .$$

Από την άλλη μεριά, εάν $r \in \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_n \rangle$, τότε $r \in \langle a_j \rangle \Longrightarrow a_j \mid r$ για κάθε $j \in \{1, \ldots, n\}$, και επειδή το t είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \ldots, a_n$, έχουμε $t \mid r \Longrightarrow r \in \langle t \rangle$, οπότε $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle \subseteq \langle t \rangle$. Κατά συνέπειαν,

$$\langle t \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_n \rangle .$$

(ii)⇒(i) Εάν υποθέσουμε ότι $\langle t \rangle = \langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle$, τότε για κάθε $j \in \{1, \ldots, n\}$ έχουμε

$$\langle t \rangle \subseteq \langle a_j \rangle \Longrightarrow a_j \mid t,$$

ενώ για οιοδήποτε $s \in R$, για το οποίο ισχύει $a_1 \mid s, \ldots, a_n \mid s$, έχουμε

$$s \in \langle a_j \rangle,\ \forall j \in \{1, \ldots, n\} \Longrightarrow s \in \langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle = \langle t \rangle \Longrightarrow t \mid s.$$

Ως εκ τούτου, το t είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \ldots, a_n$. □

5.2.25 Πόρισμα. *Οιαδήποτε πεπερασμένου πλήθους στοιχεία ενός μεταθετικού δακτυλίου κυρίων ιδεωδών R με μοναδιαίο στοιχείο διαθέτουν πάντοτε (κάποιο) ελάχιστο κοινό πολλαπλάσιο.*

5.2.26 Πόρισμα. *Έστω R μια ακεραία περιοχή. Εάν $n \in \mathbb{N},\ n \geq 2$, τα $a_1, \ldots, a_n$ στοιχεία τής R και $t \in \text{ΕΚΠ}_R(a_1, \ldots, a_n)$, τότε*

$$t = 0_R \iff \exists j \in \{1, \ldots, n\} : a_j = 0_R \iff \text{ΕΚΠ}_R(a_1, \ldots, a_n) = \{0_R\}.$$

Κατά συνέπειαν,

$$t \in R \setminus \{0_R\} \iff a_j \in R \setminus \{0_R\},\ \forall j \in \{1, \ldots, n\}.$$

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $a_j \neq 0_R$ για κάθε $j \in \{1, \ldots, n\}$. Επειδή ο θεωρηθείς δακτύλιος R είναι (εξ υποθέσεως) ακεραία περιοχή, έχουμε $\prod_{j=1}^{n} a_j \neq 0_R$. Κατά το θεώρημα 5.2.24,

$$\langle t \rangle = \langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle .$$

Παρατηρούμε ότι

$$0_R \neq \prod_{j=1}^{n} a_j \in \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_n \rangle = \langle t \rangle \Rightarrow \{0_R\} \subsetneqq \langle t \rangle \Rightarrow t \neq 0_R.$$

Εάν λοιπόν $t = 0_R$, τότε υπάρχει κατ' ανάγκην κάποιος $j \in \{1, \ldots, n\}$ με $a_j = 0_R$. Και αντιστρόφως· εάν $\exists j \in \{1, \ldots, n\} : a_j = 0_R$ και $t \in \text{ΕΚΠ}_R(a_1, \ldots, a_n)$, τότε το θεώρημα 5.2.24 μας πληροφορεί ότι

$$t \in \langle t \rangle \,(= \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_n \rangle) \subseteq \langle a_j \rangle = \langle 0_R \rangle = \{0_R\},$$

οπότε $t = 0_R$. □

5.2.27 Λήμμα. *Έστω R μια ακεραία περιοχή. Εάν $a, b \in R \setminus \{0_R\}$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Τα a, b είναι σχετικώς πρώτα.*

(ii) *Για κάθε $c \in R \setminus \{0_R\}$ με $c \mid a$ και $c \mid b$, έχουμε $c \in R^\times$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $c \in R \setminus \{0_R\}$ και $c \mid a,\ c \mid b$, τότε $c \mid 1_R$ (επειδή εξ υποθέσεως $1_R \in \text{ΜΚΔ}_R(a, b)$, βλ. 5.2.9). Αυτό σημαίνει ότι $\exists c' \in R : 1_R = cc'$, απ' όπου έπεται ότι $c \in R^\times$.

(ii)⇒(i) Έστω $c \in R$ με $c \mid a$ και $c \mid b$. Επειδή $a, b \in R \setminus \{0_R\}$, έχουμε κατ' ανάγκην $c \in R \setminus \{0_R\}$ (βλ. 5.2.3 (i)). Εξ υποθέσεως, $c \in R^\times$. Αυτό σημαίνει ότι $\exists c' \in R : 1_R = cc'$, απ' όπου έπεται ότι

$$\left.\begin{array}{r} c \mid 1_R \\ \text{5.2.3 (v)} \Rightarrow 1_R \mid a,\ 1_R \mid b \end{array}\right\} \underset{\text{5.2.9}}{\Longrightarrow} 1_R \in \text{ΜΚΔ}_R(a, b),$$

οπότε τα a, b είναι σχετικώς πρώτα. □

5.2.28 Λήμμα. *Έστω R μια ακεραία περιοχή. Εάν υποθέσουμε ότι δυο τυχόντα μη μηδενικά στοιχεία τής R διαθέτουν (κάποιον) μέγιστο κοινό διαιρέτη, τότε για $a, b, d \in R\setminus\{0_R\}$ οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) $d \in \text{ΜΚΔ}_R(a, b)$.

(ii) *Υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R\setminus\{0_R\}$, τέτοια ώστε $a = da'$ και $b = db'$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $d \in \text{ΜΚΔ}_R(a, b)$, τότε $d \mid a$ και $d \mid b$, οπότε υπάρχουν $a', b' \in R\setminus\{0_R\}$, τέτοια ώστε $a = da'$ και $b = db'$. Θα αποδείξουμε ότι τα a', b' είναι σχετικώς πρώτα. Προς τούτο θεωρούμε $c \in R$, τέτοιο ώστε $c \mid a'$ και $c \mid b'$. Τότε υπάρχουν $a'', b'' \in R\setminus\{0_R\}$ με $a' = ca''$ και $b' = cb''$. Επομένως,

$$\left.\begin{array}{r} a = dca'' \Rightarrow dc \mid a \\ b = dcb'' \Rightarrow dc \mid b \end{array}\right\} \Longrightarrow dc \mid d \Longrightarrow \exists c' \in R : d = dcc'.$$

Επειδή ο δακτύλιος αναφοράς R είναι εξ υποθέσεως ακεραία περιοχή, έχουμε

$$\left.\begin{array}{r} d(1_R - cc') = 0_R \\ d \neq 0_R \end{array}\right\} \Longrightarrow cc' = 1_R \Rightarrow c \in R^\times$$

(βλ. 1.2.5), οπότε $1_R \in \text{ΜΚΔ}_R(a', b')$ (κατόπιν εφαρμογής τού λήμματος 5.2.27 με τα a', b' στη θέση των εκεί παρατεθέντων a και b, αντιστοίχως).

(ii)⇒(i) Εξ υποθέσεως, υπάρχει κάποιος $d' \in \text{ΜΚΔ}_R(a, b)$. Επιπροσθέτως, υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R\setminus\{0_R\}$ και $d \in R\setminus\{0_R\}$, τέτοια ώστε $a = da'$ και $b = db'$. Κατά συνέπειαν,

$$\left.\begin{array}{r} d \mid a \\ d \mid b \end{array}\right\} \underset{5.2.9}{\Longrightarrow} d \mid d' \Rightarrow \exists c \in R\setminus\{0_R\} : d' = dc.$$

Εξάλλου,

$$\left.\begin{array}{r} d' \mid a \Rightarrow \exists a'' \in R\setminus\{0_R\} : da' = a = d'a'' = dca'' \\ d' \mid b \Rightarrow \exists b'' \in R\setminus\{0_R\} : db' = b = d'b'' = dcb'' \\ d \neq 0_R \end{array}\right\} \Rightarrow \left\{\begin{array}{l} a' = ca'' \\ b' = cb'' \end{array}\right\}$$

(βλ. 1.2.5), οπότε εφαρμόζοντας το λήμμα 5.2.27 (με τα a', b' στη θέση των εκεί παρατεθέντων a και b, αντιστοίχως) λαμβάνουμε

$$\left.\begin{array}{r} c \mid a',\ c \mid b' \\ 1_R \in \text{ΜΚΔ}_R(a', b') \end{array}\right\} \Longrightarrow c \in R^\times.$$

Από αυτό και από το πόρισμα 5.2.5 συνάγεται ότι $d' \underset{\text{συν.}}{\sim} d$. Το (i) τής προτάσεως 5.2.12 μας πληροφορεί ότι $d \in \text{ΜΚΔ}_R(a, b)$. □

5.2.29 Λήμμα. *Έστω R μια ακεραία περιοχή. Εάν υποθέσουμε ότι δυο τυχόντα μη μηδενικά στοιχεία τής R διαθέτουν (κάποιο) ελάχιστο κοινό πολλαπλάσιο, τότε για $a, b, t \in R\smallsetminus\{0_R\}$ οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) $t \in \text{ΕΚΠ}_R(a, b)$.

(ii) *Υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R\smallsetminus\{0_R\}$, τέτοια ώστε να ισχύουν οι ισότητες $t = aa' = bb'$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $t \in \text{ΕΚΠ}_R(a, b)$, τότε $a \mid t$ και $b \mid t$, οπότε υπάρχουν $a', b' \in R\smallsetminus\{0_R\}$, τέτοια ώστε $t = aa' = bb'$. Θα αποδείξουμε ότι τα a', b' είναι σχετικώς πρώτα στοιχεία. Προς τούτο θεωρούμε τυχόν $c \in R$ με $c \mid a'$ και $c \mid b'$. Λόγω αυτής τής επιλογής τού c υπάρχουν $x, y \in R$, τέτοια ώστε $a' = cx$ και $b' = cy$. Επειδή $a', b' \in R\smallsetminus\{0_R\}$, έχουμε κατ' ανάγκην $c, x, y \in R\smallsetminus\{0_R\}$. Επομένως,

$$\left.\begin{array}{r} t = c(ax) = c(by) \\ c \neq 0_R \end{array}\right\} \Longrightarrow ax = by$$

(βλ. 1.2.5), οπότε

$$\left.\begin{array}{r} a \mid ax \\ b \mid by = ax \end{array}\right\} \underset{5.2.20}{\Longrightarrow} t \mid ax \text{ και } t = c(ax) \Rightarrow ax \mid t.$$

Επομένως, $t \underset{\text{συν.}}{\sim} ax$ και $c \in R^\times$ (βλ. ορισμό 5.2.1 (ii) και πόρισμα 5.2.5). Εφαρμόζοντας το λήμμα 5.2.27 (με τα a', b' στη θέση των εκεί παρατεθέντων a και b, αντιστοίχως) λαμβάνουμε $1_R \in \text{ΜΚΔ}_R(a', b')$.

(ii)⇒(i) Εξ υποθέσεως, υπάρχει κάποιο $t' \in \text{ΕΚΠ}_R(a, b)$. Επιπροσθέτως, υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R\smallsetminus\{0_R\}$ και $t \in R\smallsetminus\{0_R\}$, τέτοια ώστε να ισχύουν οι ισότητες $t = aa' = bb'$. Κατά συνέπειαν,

$$\left.\begin{array}{r} a \mid t \\ b \mid t \end{array}\right\} \underset{5.2.20}{\Longrightarrow} t' \mid t \Rightarrow \exists c \in R\smallsetminus\{0_R\} : t = t'c.$$

Εξάλλου,

$$\left.\begin{array}{r} a \mid t' \Rightarrow \exists a'' \in R\smallsetminus\{0_R\} : t' = aa'' \\ b \mid t' \Rightarrow \exists b'' \in R\smallsetminus\{0_R\} : t' = bb'' \end{array}\right\} \Rightarrow \left\{\begin{array}{c} aa' = t = aa''c \\ bb' = t = bb''c \end{array}\right\}.$$

Επειδή $a, b \in R\smallsetminus\{0_R\}$, έχουμε λόγω τής προτάσεως 1.2.5 και τού λήμματος 5.2.27 (με τα a', b' στη θέση των εκεί παρατεθέντων a και b, αντιστοίχως)

$$\left.\begin{array}{r} a' = a''c \Rightarrow c \mid a' \\ b' = b''c \Rightarrow c \mid b' \\ 1_R \in \text{ΜΚΔ}_R(a', b') \end{array}\right\} \Longrightarrow c \in R^\times.$$

Από αυτό και από το πόρισμα 5.2.5 συνάγεται η σχέση συντροφικότητας $t \underset{\text{συν.}}{\sim} t'$. Το (i) τής προτάσεως 5.2.23 μας πληροφορεί ότι $t \in \text{ΕΚΠ}_R(a, b)$. □

5.2.30 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε ισχύουν τα εξής*:

(i) *Εάν υποθέσουμε ότι δυο τυχόντα μη μηδενικά στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη και εάν θεωρήσουμε $a, b \in R\setminus\{0_R\}$, τότε υπάρχει $t \in R\setminus\{0_R\}$, τέτοιο ώστε να ισχύει*

$$t \in \text{ΕΚΠ}_R(a,b) \text{ και } td = ab, \text{ όπου } d \in \text{ΜΚΔ}_R(a,b).$$

(ii) *Εάν υποθέσουμε ότι δυο τυχόντα μη μηδενικά στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο και εάν θεωρήσουμε $a, b \in R\setminus\{0_R\}$, τότε υπάρχει $d \in R\setminus\{0_R\}$, τέτοιο ώστε να ισχύει*

$$d \in \text{ΜΚΔ}_R(a,b) \text{ και } td = ab, \text{ όπου } t \in \text{ΕΚΠ}_R(a,b).$$

ΑΠΟΔΕΙΞΗ. (i) Εάν $a, b \in R\setminus\{0_R\}$ και $d \in \text{ΜΚΔ}_R(a,b)$, τότε σύμφωνα με το λήμμα 5.2.28 υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R\setminus\{0_R\}$, τέτοια ώστε $a = da'$ και $b = db'$. Θέτοντας $t := da'b'$ παρατηρούμε ότι $t = ab' = ba'$. Εφαρμόζοντας τη συνεπαγωγή (ii)⇒(i) τού λήμματος 5.2.29 (με το στοιχείο a στη θέση τού εκεί παρατεθέντος b και το στοιχείο b στη θέση τού εκεί παρατεθέντος a) διαπιστώνουμε ότι $t \in \text{ΕΚΠ}_R(b,a) = \text{ΕΚΠ}_R(a,b)$. Επιπροσθέτως, εξ ορισμού τού t έχουμε $td = ab$.

(ii) Εάν $a, b \in R\setminus\{0_R\}$ και $t \in \text{ΕΚΠ}_R(a,b)$, τότε σύμφωνα με το λήμμα 5.2.29 υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R\setminus\{0_R\}$, τέτοια ώστε $t = aa' = bb'$. Επειδή $a \mid ab$ και $b \mid ab$, από τον ορισμό 5.2.20 τού ελαχίστου κοινού πολλαπλασίου έπεται ότι $t \mid ab$. Κατά συνέπειαν, $\exists d \in R\setminus\{0_R\}$, τέτοιο ώστε να ισχύει $ab = td$, οπότε

$$\left.\begin{array}{l} ab = td = aa'd \\ ba = td = bb'd \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} b = a'd = da' \\ a = b'd = db' \end{array}\right\},$$

καθότι ο θεωρηθείς δακτύλιος R είναι εξ υποθέσεως ακεραία περιοχή (βλ. 1.2.5). Επειδή τα a', b' είναι σχετικώς πρώτα, εφαρμόζοντας τη συνεπαγωγή (ii)⇒(i) τού λήμματος 5.2.28 διαπιστώνουμε ότι $d \in \text{ΜΚΔ}_R(a,b)$. □

5.2.31 Λήμμα. *Έστω R μια ακεραία περιοχή. Εάν δυο τυχόντα στοιχεία τής R διαθέτουν πάντοτε κάποιον μέγιστο κοινό διαιρέτη και $a_1, a_2, a_3 \in R$, τότε*

$$\text{ΜΚΔ}_R(a_1,a_2,a_3) = \text{ΜΚΔ}_R(d,a_3),\ \forall d \in \text{ΜΚΔ}_R(a_1,a_2). \tag{5.12}$$

(*Ως εκ τούτου,* $\text{ΜΚΔ}_R(a_1,a_2,a_3) \neq \varnothing$.)

ΑΠΟΔΕΙΞΗ. Θεωρούμε τυχόντες μεγίστους κοινούς διαιρέτες $d \in \text{ΜΚΔ}_R(a_1,a_2)$, $d' \in \text{ΜΚΔ}_R(d,a_3)$, καθώς και τυχόν $c \in R$ με $c \mid a_j$ για κάθε $j \in \{1,2,3\}$. Προφανώς,

$$\left.\begin{array}{r} d' \mid d \text{ και } d \mid a_1,\ d \mid a_2 \Rightarrow d' \mid a_1 \text{ και } \begin{array}{l} d' \mid a_2 \\ d' \mid a_3 \end{array} \end{array}\right\} \Rightarrow d' \mid a_j, \forall j \in \{1,2,3\}. \tag{5.13}$$

Από τον ορισμό 5.2.9 (εφαρμοζόμενον τόσον για τον d όσον και για τον d') λαμβάνουμε

$$c \mid a_1 \text{ και } c \mid a_2 \Rightarrow c \mid d, \quad c \mid d \text{ και } c \mid a_3 \Rightarrow c \mid d'. \tag{5.14}$$

Από τις (5.13) και (5.14) συμπεραίνουμε ότι $d' \in \text{ΜΚΔ}_R(a_1, a_2, a_3)$. Επομένως,

$$\text{ΜΚΔ}_R(a_1, a_2, a_3) \neq \varnothing \text{ και } \text{ΜΚΔ}_R(d, a_3) \subseteq \text{ΜΚΔ}_R(a_1, a_2, a_3).$$

Έστω τώρα τυχών $d'' \in \text{ΜΚΔ}_R(a_1, a_2, a_3)$. Από τον ορισμό 5.2.9 γνωρίζουμε ότι ισχύουν οι σχέσεις διαιρετότητας

$$d'' \mid a_1 \text{ και } d'' \mid a_2 \Rightarrow d'' \mid d, \quad d'' \mid d \text{ και } d'' \mid a_3 \Rightarrow d'' \mid d',$$

από τη μια μεριά και οι σχέσεις διαιρετότητας

$$\left.\begin{array}{r} d' \mid d \text{ και } d \mid a_1,\ d \mid a_2 \Rightarrow d' \mid a_1 \text{ και } d' \mid a_2 \\ d' \mid a_3 \\ d'' \in \text{ΜΚΔ}_R(a_1, a_2, a_3) \end{array}\right\} \Rightarrow d' \mid d'',$$

από την άλλη. Αυτό σημαίνει ότι $d' \underset{\text{συν.}}{\sim} d''$. Από την πρόταση 5.2.12 συνάγεται ότι $d' \in \text{ΜΚΔ}_R(a_1, a_2, a_3)$ και $d'' \in \text{ΜΚΔ}_R(d, a_3)$, απ' όπου έπεται ότι η (5.12) είναι αληθής. □

5.2.32 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε ισχύουν τα ακόλουθα*:

(i) *Εάν δυο τυχόντα στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη, τότε και οιαδήποτε πεπερασμένου πλήθους στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη.*

(ii) *Εάν δυο τυχόντα στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο, τότε και οιαδήποτε πεπερασμένου πλήθους στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο.*

(iii) *Εάν δυο τυχόντα στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη, τότε και δυο τυχόντα στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο, και τανάπαλιν.*

(iv) *Εάν οιαδήποτε πεπερασμένου πλήθους στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη, τότε και οιαδήποτε πεπερασμένου πλήθους στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο, και τανάπαλιν.*

ΑΠΟΔΕΙΞΗ. (i) Εάν $n \in \mathbb{N}$, $n \geq 3$, και εάν τα $a_1, a_2, \ldots, a_n$ είναι στοιχεία τού R, τότε -εξ υποθέσεως- οιοδήποτε ζεύγος εξ αυτών διαθέτει κάποιον μέγιστο κοινό διαιρέτη. Θα αποδείξουμε ότι ο ισχυρισμός είναι αληθής μέσω μαθηματικής επαγωγής. Έστω $n = 3$ και έστω $d \in \text{ΜΚΔ}_R(a_1, a_2)$. Εάν $d' \in \text{ΜΚΔ}_R(d, a_3)$, τότε σύμφωνα με το λήμμα 5.2.31 έχουμε

$$d' \in \text{ΜΚΔ}_R(a_1, a_2, a_3).$$

Εν συνεχεία, υποθέτουμε ότι $n \geq 4$ και ότι ο ισχυρισμός μας είναι αληθής για τα $a_1, \ldots, a_{n-1}$. Έστω $d \in \text{ΜΚΔ}_R(a_1, \ldots, a_{n-1})$. Εξ υποθέσεως, $\exists d' \in \text{ΜΚΔ}_R(d, a_n)$. Έστω $c \in R$ με $c \mid a_j$ για κάθε $j \in \{1, \ldots, n\}$. Προφανώς,

$$\left.\begin{array}{r} d' \mid d \text{ και } d \mid a_j,\ \forall j \in \{1, \ldots, n-1\} \\ \Rightarrow d \mid a_j,\ \forall j \in \{1, \ldots, n-1\} \\ d' \mid a_n \end{array}\right\} \Rightarrow d' \mid a_j, \forall j \in \{1, \ldots, n\}. \qquad (5.15)$$

Από τον ορισμό 5.2.9 (εφαρμοζόμενον τόσον για τον d όσον και για τον d') λαμβάνουμε

$$c \mid a_j,\ \forall j \in \{1, \ldots, n-1\} \Rightarrow\ c \mid d, \quad c \mid d \text{ και } c \mid a_n \Rightarrow\ c \mid d'. \qquad (5.16)$$

Από τις (5.15) και (5.16) συμπεραίνουμε ότι $d' \in \text{ΜΚΔ}_R(a_1, \ldots, a_{n-1}, a_n)$. Επομένως,

$$\text{ΜΚΔ}_R(a_1, \ldots, a_n) \neq \varnothing \text{ και } \text{ΜΚΔ}_R(d, a_n) \subseteq \text{ΜΚΔ}_R(a_1, \ldots, a_n).$$

(Με επιχειρήματα ανάλογα εκείνων που χρησιμοποιήθησαν στο λήμμα 5.2.31, όπου $n = 3$, μπορεί κανείς να δείξει ότι $\text{ΜΚΔ}_R(d, a_n) = \text{ΜΚΔ}_R(a_1, \ldots, a_n)$, αλλά εδώ αρκεί μόνον η διασφάλιση τής υπάρξεως *τουλάχιστον ενός* μεγίστου κοινού διαιρέτη των $a_1, \ldots, a_n$).

(ii) Εάν $n \in \mathbb{N}$, $n \geq 3$, και εάν τα $a_1, a_2, \ldots, a_n$ είναι στοιχεία τού R, τότε -εξ υποθέσεως- οιοδήποτε ζεύγος εξ αυτών διαθέτει κάποιο ελάχιστο κοινό πολλαπλάσιο. Θα αποδείξουμε ότι ο ισχυρισμός είναι αληθής μέσω μαθηματικής επαγωγής. Έστω $n = 3$ και έστω $t \in \text{ΕΚΠ}_R(a_1, a_2)$. Τότε

$$\langle t \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \Longrightarrow \langle t \rangle \cap \langle a_3 \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \langle a_3 \rangle$$

και επειδή τα t και a_3 διαθέτουν κάποιο ελάχιστο κοινό πολλαπλάσιο, ας το πούμε t', με $\langle t' \rangle = \langle t \rangle \cap \langle a_3 \rangle$ (βλ. 5.2.24 (i)⇒(ii)), έχουμε

$$\langle t' \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \langle a_3 \rangle .$$

Τούτο σημαίνει ότι το t' είναι κατ' ανάγκην ένα ελάχιστο κοινό πολλαπλάσιο των a_1, a_2, a_3 (λόγω τού 5.2.24 (ii)⇒(i)). Εν συνεχεία, υποθέτουμε ότι $n \geq 4$ και ότι ο ισχυρισμός μας είναι αληθής για τα $a_1, \ldots, a_{n-1}$. Εάν το t είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, \ldots, a_{n-1}$, τότε

$$\langle t \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_{n-1} \rangle \Longrightarrow \langle t \rangle \cap \langle a_n \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_n \rangle ,$$

και επειδή τα t και a_n διαθέτουν (εξ υποθέσεως) κάποιο ελάχιστο κοινό πολλαπλάσιο, ας το πούμε t', με $\langle t' \rangle = \langle t \rangle \cap \langle a_n \rangle$ (βλ. 5.2.24 (i)⇒(ii)), έχουμε

$$\langle t' \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \langle a_3 \rangle \cap \cdots \cap \langle a_{n-1} \rangle \cap \langle a_n \rangle ,$$

κάτι που σημαίνει ότι το t' είναι κατ' ανάγκην ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \ldots, a_n$ (λόγω τού 5.2.24 (ii)⇒(i)).

(iii) Κατ' αρχάς, υποθέτοντας ότι δυο τυχόντα στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη, θα αποδείξουμε ότι $\text{ΕΚΠ}_R(a,b) \neq \varnothing$ για οιαδήποτε $a, b \in R$. Εάν τουλάχιστον ένα εκ των a, b είναι $= 0_R$, τότε έχουμε $\text{ΕΚΠ}_R(a,b) = \{0_R\} \neq \varnothing$ (βλ. πόρισμα 5.2.26). Εάν $a, b \in R \smallsetminus \{0_R\}$, τότε η ύπαρξη κάποιου μεγίστου κοινού διαιρέτη $d \in \text{ΜΚΔ}_R(a,b)$ συνεπιφέρει την ύπαρξη ενός $t \in \text{ΕΚΠ}_R(a,b)$ με $td = ab$ επί τη βάσει τής προτάσεως 5.2.30.

Εν συνεχεία, υποθέτοντας ότι δυο τυχόντα στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο, θα αποδείξουμε ότι $\text{ΜΚΔ}_R(a,b) \neq \varnothing$ για οιαδήποτε $a, b \in R$. Εάν $a = 0_R$, τότε προφανώς $b \in \text{ΜΚΔ}_R(0_R, b)$. Κατ' αναλογίαν, εάν $b = 0_R$, τότε $a \in \text{ΜΚΔ}_R(a, 0_R)$. Εάν $a, b \in R \smallsetminus \{0_R\}$, τότε η ύπαρξη κάποιου ελαχίστου κοινού πολλαπλασίου $t \in \text{ΕΚΠ}_R(a,b)$ συνεπιφέρει την ύπαρξη ενός $d \in \text{ΜΚΔ}_R(a,b)$ με $td = ab$ επί τη βάσει τής προτάσεως 5.2.30.

(iv) Τούτο έπεται άμεσα από τα (i), (ii) και (iii). □

5.2.33 Ορισμός. Έστω R μια ακεραία περιοχή. Η R καλείται **περιοχή με μέγιστο κοινό διαιρέτη** ή, εν συντομία, **περιοχή με μ.κ.δ.** όταν $\text{ΜΚΔ}_R(a,b) \neq \varnothing$ για οιαδήποτε στοιχεία $a, b \in R$. (Εάν η R είναι περιοχή με μ.κ.δ., τότε, βάσει τής προτάσεως 5.2.32, και οιαδήποτε πεπερασμένου πλήθους στοιχεία τής R διαθέτουν τόσο μέγιστο κοινό διαιρέτη όσο και ελάχιστο κοινό πολλαπλάσιο).

5.2.34 Παράδειγμα. Κάθε Π.Κ.Ι. είναι περιοχή με μ.κ.δ. (Βλ. πόρισμα 5.2.15 ή, εναλλακτικώς, το πόρισμα 5.6.8 σε συνδυασμό με το θεώρημα 5.6.13.)

5.2.35 Πρόταση. *Έστω R μια περιοχή με μ.κ.δ. Εάν $a, b, c \in R$, τότε ισχύουν τα ακόλουθα*:

(i) $a \in \text{ΜΚΔ}_R(a,a)$,

(ii) $a \mid b \iff a \in \text{ΜΚΔ}_R(a,b)$,

(iii) $\text{ΜΚΔ}_R(d,c) = \text{ΜΚΔ}_R(a,d')$, $\forall d \in \text{ΜΚΔ}_R(a,b)$ *και* $\forall d' \in \text{ΜΚΔ}_R(b,c)$,

(iv) $\text{ΜΚΔ}_R(ca,cb) = \{\, cd \mid d \in \text{ΜΚΔ}_R(a,b)\}$,

(v) $\text{ΜΚΔ}_R(ab,c) = \text{ΜΚΔ}_R(db,c)$, *για οιονδήποτε* $d \in \text{ΜΚΔ}_R(a,c)$.

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $a \mid a$ και για κάθε $c \in R$ με $c \mid a$ ικανοποιούνται οι συνθήκες τού ορισμού 5.2.9 για το a, οπότε $a \in \text{ΜΚΔ}_R(a,a)$.

(ii) Υποθέτοντας ότι $a \mid b$, έχουμε $a \mid a$ και $a \mid b$, και για κάθε $c \in R$ με $c \mid a$ και $c \mid b$ ικανοποιούνται οι συνθήκες τού ορισμού 5.2.9 για το a, οπότε $a \in \text{ΜΚΔ}_R(a,b)$. Το αντίστροφο είναι προφανές.

(iii) Θεωρούμε τυχόντες $d \in \text{ΜΚΔ}_R(a,b)$, $d' \in \text{ΜΚΔ}_R(b,c)$. Εάν $d'' \in \text{ΜΚΔ}_R(d,c)$ και $d''' \in \text{ΜΚΔ}_R(a,d')$, αρκεί να δειχθεί ότι[5] $d'' \underset{\text{συν.}}{\sim} d'''$, ήτοι ότι $d'' \mid d'''$ και $d''' \mid d''$. Εξ υποθέσεως, $d'' \mid d$ και $d'' \mid c$. Επειδή $d \mid a$ και $d \mid b$, έχουμε $d'' \mid a$, $d'' \mid b$ και $d'' \mid c$. Από την άλλη μεριά, επειδή $d' \in \text{ΜΚΔ}_R(b,c)$, έχουμε

$$\left.\begin{array}{r} d'' \mid a \ \text{ και } \ d'' \mid d' \\ d''' \in \text{ΜΚΔ}_R(a,d') \end{array}\right\} \Rightarrow d'' \mid d'''.$$

Η σχέση διαιρετότητας $d''' \mid d''$ αποδεικνύεται παρομοίως.

(iv) Εάν $d \in \text{ΜΚΔ}_R(a,b)$ και $d' \in \text{ΜΚΔ}_R(ca,cb)$, αρκεί να δειχθεί ότι $d' \underset{\text{συν.}}{\sim} cd$, ήτοι ότι $d' \mid cd$ και $cd \mid d'$. Εάν $c = 0_R$, τούτο είναι προφανές, διότι

$$\text{ΜΚΔ}_R(0_R, 0_R) = \{0_R\}.$$

Εάν $c \neq 0_R$, τότε από τις σχέσεις διαιρετότητας $d \mid a$ και $d \mid b$ έπονται άμεσα οι $cd \mid ca$ και $cd \mid cb$ (βλ. 5.2.3 (ii)), οπότε $cd \mid d'$. Εξάλλου,

$$\left.\begin{array}{r} cd \mid d' \Rightarrow \exists r \in R : d' = (cd)\, r \\ d' \mid ca \Rightarrow \exists s \in R : ca = d's \\ d' \mid cb \Rightarrow \exists t \in R : cb = d't \end{array}\right\} \Rightarrow ca = cdrs,\ cb = cdrt.$$

Επειδή ο θεωρηθείς δακτύλιος R είναι εξ υποθέσεως ακεραία περιοχή, έχουμε

$$\left.\begin{array}{r} a = drs \\ b = drt \end{array}\right\} \Rightarrow dr \mid a \ \text{ και } \ dr \mid b$$

(βλ. 1.2.5), οπότε $d \in \text{ΜΚΔ}_R(a,b) \Rightarrow dr \mid d \Rightarrow d' = c\,(dr) \mid cd$.

(v) Έστω τυχών $d \in \text{ΜΚΔ}_R(a,c)$. Κατά το (iv), $db \in \text{ΜΚΔ}_R(ab,cb)$. Έστω τυχών $d' \in \text{ΜΚΔ}_R(ab,cb)$. Τότε $d \underset{\text{συν.}}{\sim} d'$, οπότε

$$\left.\begin{array}{r} \text{ΜΚΔ}_R(db,c) = \text{ΜΚΔ}_R(d',c) \\ \text{(iii)} \Rightarrow \text{ΜΚΔ}_R(d',c) = \text{ΜΚΔ}_R(ab,d''), \\ \forall d'' \in \text{ΜΚΔ}_R(cb,c) \end{array}\right\} \Rightarrow \left\{\begin{array}{c} \text{ΜΚΔ}_R(db,c) = \text{ΜΚΔ}_R(ab,d''), \\ \forall d'' \in \text{ΜΚΔ}_R(cb,c) \end{array}\right\}$$

Κατά το (ii), $c \in \text{ΜΚΔ}_R(cb,c)$. Επιλέγοντας λοιπόν ως d'' το c, λαμβάνουμε $\text{ΜΚΔ}_R(db,c) = \text{ΜΚΔ}_R(ab,c)$. □

Ανάλογες ιδιότητες που αφορούν στα σύνολα των ελαχίστων κοινών πολλαπλασίων περιλαμβάνονται στην ακόλουθη πρόταση:

5.2.36 Πρόταση. *Έστω R μια περιοχή με μ.κ.δ. Εάν $a,b,c \in R$, τότε ισχύουν τα ακόλουθα*:

[5] Εάν $d'' \underset{\text{συν.}}{\sim} d'''$, τότε από την πρόταση 5.2.12 συνάγουμε ότι $d''' \in \text{ΜΚΔ}_R(d,c)$ και $d'' \in \text{ΜΚΔ}_R(a,d')$, οπότε $\text{ΜΚΔ}_R(d,c) = \text{ΜΚΔ}_R(a,d')$.

(i) $a \in \text{ΕΚΠ}_R(a,a)$,

(ii) $a \mid b \iff b \in \text{ΕΚΠ}_R(a,b)$,

(iii) $\text{ΕΚΠ}_R(t,c) = \text{ΕΚΠ}_R(a,t'), \forall t \in \text{ΕΚΠ}_R(a,b)$ *και* $\forall t' \in \text{ΕΚΠ}_R(b,c)$,

(iv) $\text{ΕΚΠ}_R(ca,cb) = \{\, ct \mid t \in \text{ΕΚΠ}_R(a,b)\}$,

(v) $\text{ΕΚΠ}_R(ab,c) = \text{ΕΚΠ}_R(tb,c)$, *για οιοδήποτε* $t \in \text{ΕΚΠ}_R(a,c)$.

Επιπροσθέτως, η πρόταση 5.2.19 εξακολουθεί να ισχύει και για περιοχές με μ.κ.δ.

5.2.37 Πρόταση. *Έστω R μια περιοχή με μ.κ.δ. Εάν $a,b,c \in R$, τότε ισχύουν τα εξής:*

(i) *Εάν $a \mid bc$ και τα a,b είναι σχετικώς πρώτα, τότε $a \mid c$.*

(ii) *Εάν $a \mid c$, $b \mid c$ και τα a,b είναι σχετικώς πρώτα, τότε $ab \mid c$.*

(iii) *Εάν $c \mid a$ και τα a,b είναι σχετικώς πρώτα, τότε και τα c και b είναι σχετικώς πρώτα.*

► **Παράδειγμα ακεραίας περιοχής που δεν είναι περιοχή με μ.κ.δ.** Για την εύρεση παραδειγμάτων ακεραίων περιοχών που δεν είναι περιοχές με μ.κ.δ. θα εργασθούμε εντός τής κλάσεως των τετραγωνικών αριθμητικών περιοχών $\mathbb{Z}[\sqrt{m}]$ για κατάλληλους ακεραίους m στερούμενους τετραγώνων (βλ. άσκηση **1-44**). Συγκεκριμένα, στην πρόταση 5.2.43 θα αποδείξουμε ότι η $\mathbb{Z}[\sqrt{-5}]$ δεν είναι περιοχή με μ.κ.δ. Εν συνεχεία (στην πρόταση 5.3.8) θα καταλήξουμε στο ίδιο συμπέρασμα για τετραγωνικές αριθμητικές περιοχές $\mathbb{Z}[\sqrt{m}]$ αντιστοιχιζόμενες σε *απείρου πλήθους* ακεραίους m. Προτάσσουμε τον ορισμό τής *αριθμητικής στάθμης* τού $\mathbb{Q}(\sqrt{m})$, καθώς και τις βασικές ιδιότητες αυτής (οι οποίες, όπως θα διαπιστώσουμε τόσο στην παρούσα όσον και στις επόμενες ενότητες, υπεισέρχονται κατά τρόπο ουσιαστικό σε πληθώρα λίαν χρήσιμων εφαρμογών).

5.2.38 Ορισμός. Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων και έστω $\mathbb{Q}(\sqrt{m}) \subsetneqq \mathbb{C}$ το τετραγωνικό αριθμητικό σώμα το αντιστοιχιζόμενο σε αυτόν. Εάν $z = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ $(x,y \in \mathbb{Q})$, τότε λέμε ο $\overline{z} := x - y\sqrt{m}$ είναι ο **συζυγής**[6] τού z. Ως **αριθμητική στάθμη** τού $\mathbb{Q}(\sqrt{m})$ ορίζουμε την απεικόνιση

[6] Όταν $m \leq -1$, τότε ο $\overline{z}$ είναι ο συζυγής τού $z \in \mathbb{C}$ *υπό τη συνήθη έννοια*:

$$x =: \mathrm{Re}(z), y\sqrt{m} = yi\sqrt{|m|} =: \mathrm{Im}(z) \text{ και } \overline{z} := \mathrm{Re}(z) - \mathrm{Im}(z).$$

Όταν $m \geq 2$, τότε $z \in \mathbb{R}$ και "κατ' αναλογίαν" ο $x =: \mathrm{Rat}(z) \in \mathbb{Q}$ μπορεί να εκληφθεί ως το *ρητό μέρος* τού z και ο $y\sqrt{m} =: \mathrm{Irr}(z) \in \mathbb{R} \setminus \mathbb{Q}$ ως το *άρρητο μέρος* τού z, με τον $\overline{z} := \mathrm{Rat}(z) - \mathrm{Irr}(z)$ ως συζυγή του. Σημειωτέον ότι

$$\boxed{z + \overline{z} = \begin{cases} 2\,\mathrm{Rat}(z), & \text{όταν } m \geq 2, \\ 2\,\mathrm{Re}(z), & \text{όταν } m \leq -1, \end{cases}} \text{ και } \boxed{z - \overline{z} = \begin{cases} 2\,\mathrm{Irr}(z), & \text{όταν } m \geq 2, \\ 2\,\mathrm{Im}(z), & \text{όταν } m \leq -1. \end{cases}}$$

$\mathbf{N} : \mathbb{Q}(\sqrt{m}) \longrightarrow \mathbb{Q}$ μέσω τού τύπου

$$\boxed{\mathbf{N}(z) := z\overline{z} = (x + y\sqrt{m})(x - y\sqrt{m}) = x^2 - my^2,}$$

για κάθε $z = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ $(x, y \in \mathbb{Q})$.

5.2.39 Πρόταση. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν $z, w \in \mathbb{Q}(\sqrt{m})$, τότε η αριθμητική στάθμη $\mathbf{N}$ τού τετραγωνικού αριθμητικού σώματος $\mathbb{Q}(\sqrt{m})$ έχει τις εξής ιδιότητες*:

(i) $\mathbf{N}(z) = 0 \Longleftrightarrow z = 0$.

(ii) $\mathbf{N}(zw) = \mathbf{N}(z)\,\mathbf{N}(w)$ *και* $|\mathbf{N}(zw)| = |\mathbf{N}(z)|\,|\mathbf{N}(w)|$.

(iii) *Εάν* $z \mid w$, *τότε* $\mathbf{N}(z) \mid \mathbf{N}(w)$ *και* $|\mathbf{N}(z)| \mid |\mathbf{N}(w)|$.

(iv) $z \in \mathbb{Z}[\sqrt{m}] \Rightarrow \mathbf{N}(z) \in \mathbb{Z}$.

(v) $z \in \mathbb{Z}[\sqrt{m}], m < 0 \Rightarrow \mathbf{N}(z) \in \mathbb{N}_0$.

(vi) $z \in \mathbb{Z}[\sqrt{m}]^{\times} \Longleftrightarrow \mathbf{N}(z) \in \{\pm 1\}$.

(vii) *Εάν* $z, w \in \mathbb{Z}[\sqrt{m}]$ *και* $z \underset{\text{συν.}}{\sim} w$, *τότε* $|\mathbf{N}(z)| = |\mathbf{N}(w)|$.

ΑΠΟΔΕΙΞΗ. (i) Εάν $z = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ $(x, y \in \mathbb{Q})$ με $\mathbf{N}(z) = 0$, τότε $y = 0$, διότι υποθέτοντας ότι $y \neq 0$, καταλήγουμε σε αντίφαση:

$$x^2 - my^2 = 0 \Longrightarrow m = \left(\frac{x}{y}\right)^2 \Longrightarrow \sqrt{m} \in \mathbb{Q},$$

Επομένως, $y = 0 \Rightarrow \mathbf{N}(z) = x^2 = 0 \Rightarrow x = 0 \Rightarrow z = 0$. Το αντίστροφο είναι προφανές.

(ii) Εάν

$$z = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m}),\ w = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})\ \ (r, s, x, y \in \mathbb{Q}),$$

τότε $zw = (rx + msy) + (ry + sx)\sqrt{m}$, οπότε

$$\begin{aligned} \mathbf{N}(zw) &= (rx + msy)^2 - m(ry + sx)^2 \\ &= r^2x^2 + m^2s^2y^2 - mr^2y^2 - ms^2x^2 \\ &= \left(r^2 - ms^2\right)\left(x^2 - my^2\right) = \mathbf{N}(z)\,\mathbf{N}(w). \end{aligned}$$

Η ισότητα $|\mathbf{N}(zw)| = |\mathbf{N}(z)|\,|\mathbf{N}(w)|$ είναι προφανής.

(iii) Τούτο έπεται άμεσα από το (ii).

(iv) Εάν $z = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ $(a, b \in \mathbb{Z})$, τότε

$$a, b, m \in \mathbb{Z} \Longrightarrow \mathbf{N}(z) = a^2 - mb^2 \in \mathbb{Z}.$$

(v) Εάν $z = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ $(a, b \in \mathbb{Z})$ και $m < 0$, τότε

$$a^2 \geq 0,\ b^2 \geq 0,\ -m > 0 \Longrightarrow \mathbf{N}(z) = a^2 - mb^2 \in \mathbb{N}_0.$$

(vi) Εάν $z \in \mathbb{Z}[\sqrt{m}]^{\times}$, τότε από το (ii) έπεται ότι

$$\left.\begin{array}{r} 1 = \mathbf{N}(1) = \mathbf{N}\left(zz^{-1}\right) = \mathbf{N}(z)\,\mathbf{N}\left(z^{-1}\right) \\ \text{(iii)} \Longrightarrow \mathbf{N}(z) \in \mathbb{Z},\ \mathbf{N}\left(z^{-1}\right) \in \mathbb{Z} \end{array}\right\} \Longrightarrow \mathbf{N}(z) \in \{\pm 1\}.$$

Και αντιστρόφως· εάν $z = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ $(a, b \in \mathbb{Z})$ με

$$\mathbf{N}(z) = a^2 - mb^2 \in \{\pm 1\},$$

τότε

$$z(\mathbf{N}(z)\,\overline{z}) = (a + b\sqrt{m})(\mathbf{N}(z)\left(a - b\sqrt{m}\right)) = \mathbf{N}(z)^2 = 1,$$

οπότε το z έχει το $\mathbf{N}(z)\,\overline{z}$ ως αντίστροφό του.

(vii) Εάν $z, w \in \mathbb{Z}[\sqrt{m}]$ και $z \underset{\text{συν.}}{\sim} w$, τότε $z = uw$ για κάποιο $u \in \mathbb{Z}[\sqrt{m}]^{\times}$ (βλ. πόρισμα 5.2.5). Από τα (ii) και (vi) έπεται ότι

$$\mathbf{N}(z) = \mathbf{N}(uw) = \mathbf{N}(u)\,\mathbf{N}(w) \in \{\pm\mathbf{N}(w)\},$$

οπότε $|\mathbf{N}(z)| = |\mathbf{N}(w)|$. □

5.2.40 Παρατήρηση. Ως γνωστόν, $\mathbb{Q}(\sqrt{m}) = \mathbf{Fr}(\mathbb{Z}[\sqrt{m}])$ (βλ. άσκηση **3-47**). Εάν λοιπόν $z = \frac{u}{w} \in \mathbb{Q}(\sqrt{m})$, όπου $(u, w) \in \mathbb{Z}[\sqrt{m}] \times (\mathbb{Z}[\sqrt{m}] \smallsetminus \{0\})$, τότε λόγω των ιδιοτήτων 5.2.39 (i) και (ii) έχουμε

$$u = zw \Rightarrow \mathbf{N}(u) = \mathbf{N}(zw) = \mathbf{N}(z)\,\mathbf{N}(w) \Rightarrow \mathbf{N}(z) = \tfrac{\mathbf{N}(u)}{\mathbf{N}(w)}.$$

5.2.41 Σημείωση. (Περί τής ομάδας των αντιστρεψίμων στοιχείων.)
Με τη βοήθεια τής ιδιότητας 5.2.39 (vi) είναι δυνατός ο ακριβής προσδιορισμός τής ομάδας $\mathbb{Z}[\sqrt{m}]^{\times}$ των αντιστρεψίμων στοιχείων τής τετραγωνικής αριθμητικής περιοχής $\mathbb{Z}[\sqrt{m}]$. Ένα στοιχείο $z = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ $(a, b \in \mathbb{Z})$, ανήκει στην $\mathbb{Z}[\sqrt{m}]^{\times}$ εάν και μόνον εάν το διατεταγμένο ζεύγος (a, b) ανήκει στο σύνολο των $(x, y) \in \mathbb{Z}^2$ που ικανοποιούν είτε τη διοφαντική εξίσωση

$$\boxed{x^2 - my^2 = 1} \tag{5.17}$$

είτε τη διοφαντική εξίσωση

$$\boxed{x^2 - my^2 = -1.} \tag{5.18}$$

(Διοφαντικές εξισώσεις αυτού τού τύπου καλούνται **εξισώσεις τού Pell**.) Διακρίνουμε δύο περιπτώσεις:

(i) Εάν $m \leq -1$, τότε η (5.18) δεν διαθέτει καμία ακεραία λύση (αφού $x^2 - my^2 \geq 0$ για κάθε $(x, y) \in \mathbb{Z}^2$), ενώ οι μόνες ακέραιες λύσεις τής (5.17) είναι οι $(\pm 1, 0)$ όταν

$m<-1$ (αφού $y\neq 0\Rightarrow x^2-my^2>1$) και οι $(\pm 1,0),(0,\pm 1)$ όταν $m=-1$ (αφού έχουμε κατ' ανάγκην $xy=0$). Επομένως,

$$\boxed{\mathbb{Z}[\sqrt{m}]^{\times}=\begin{cases}\{\pm 1\}, & \text{όταν } m<-1,\\ \{\pm 1,\pm i\}, & \text{όταν } m=-1.\end{cases}}$$

(ii) Εάν $m\geq 2$, τότε

$$\boxed{\mathbb{Z}[\sqrt{m}]^{\times}=\{x+y\sqrt{m}\mid (x,y)\in \Lambda_{+1}(m)\cup\Lambda_{-1}(m)\},} \tag{5.19}$$

όπου το σύνολο $\Lambda_{+1}(m):=\left\{(x,y)\in\mathbb{Z}\times\mathbb{Z}|\, x^2-my^2=1\right\}$ των ακεραίων λύσεων τής (5.17) είναι πάντοτε μη κενό (περιέχον προδήλως τις «τετριμμένες» λύσεις $(\pm 1,0)$), ενώ το σύνολο

$$\Lambda_{-1}(m):=\left\{(x,y)\in\mathbb{Z}\times\mathbb{Z}|\, x^2-my^2=-1\right\}$$

των ακεραίων λύσεων τής (5.18) είναι άλλοτε κενό και άλλοτε μη κενό. Συγκεκριμένα, αναπτύσσοντας τη ρίζα $\sqrt{m}$ τού m ως *συνεχές κλάσμα*

$$\sqrt{m}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{\ddots\;\cfrac{}{a_{n-1}+\frac{1}{a_n+\frac{1}{\ddots}}}}}}}$$

(με άπειρους όρους $a_j\in\mathbb{N},\ j=0,1,...$) και ορίζοντας τις αναδρομικές ακολουθίες

$$p_0:=a_0=\lfloor\sqrt{m}\rfloor,\ \ p_1:=a_0a_1+1,\ \ p_n:=a_np_{n-1}+p_{n-2},$$
$$q_0:=1,\ \ q_1:=a_1,\ \ q_n:=a_nq_{n-1}+q_{n-2},\ n=2,3,...$$

όπου $p_n,q_n\in\mathbb{N}$ με μκδ$(p_n,q_n)=1$, λαμβάνουμε[7]

$$\frac{p_n}{q_n}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots\;\cfrac{}{a_{n-1}+\frac{1}{a_n}}}}}$$

με $\lim_{n\to\infty}\frac{p_n}{q_n}=\sqrt{m}$. Ο n-οστός όρος τής ακολουθίας $a_0,a_1,...,a_n,a_{n+1},...$ είναι ο $a_n=\left\lfloor\frac{a_0+P_n}{Q_n}\right\rfloor$ και υπολογίζεται από τον πρώτο της όρο a_0 μέσω των αναδρομικών

[7] Λέμε ότι ο $\frac{p_n}{q_n}$ είναι ο *n-οστός ρητός* αριθμός *ο συγκλίνων* στη ρίζα $\sqrt{m}$.

ακολουθιών

$$P_0 := 0,\ \ P_1 := a_0,\ \ P_n := a_{n-1}Q_{n-1} - P_{n-1},$$
$$Q_0 := 1,\ \ Q_1 := m - a_0^2,\ \ Q_n := \tfrac{1}{Q_{n-1}}(m - P_n^2),\ n = 2, 3, ...$$

Σημειωτέον ότι για κάθε $n \in \mathbb{N}$ ισχύουν οι ισότητες:

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1},\ \ p_n^2 - m q_n^2 = (-1)^{n+1} Q_{n+1}.$$

Από τη Θεωρία Αριθμών είναι γνωστό[8] ότι η ακολουθία $a_0, a_1, ..., a_n, a_{n+1}, ...$ είναι *περιοδική*, και μάλιστα τέτοια, ώστε $a_{\ell+n} = a_n$ *για κάθε* $n \geq 1$ (όπου ℓ το μήκος τής περιόδου της). Γι' αυτό είθισται να χρησιμοποιείται και ο εναλλακτικός (συνοπτικότερος) συμβολισμός

$$\sqrt{m} = [a_0; \overline{a_1, ..., a_\ell}],$$

όπου κάτω από την παύλα τοποθετείται η περίοδος. Επιπροσθέτως, το διατεταγμένο ζεύγος

$$\boxed{(x_1, y_1) := \begin{cases} (p_{\ell-1}, q_{\ell-1}), & \text{όταν } \ell \equiv 0 (\mathrm{mod}\, 2), \\ (p_{2\ell-1}, q_{2\ell-1}), & \text{όταν } \ell \equiv 1 (\mathrm{mod}\, 2), \end{cases}}$$

είναι το στοιχείο τού $\Lambda_{+1}(m)$ με την *ελάχιστη δυνατή θετική τετμημένη* (άρα και με την ελάχιστη θετική *τεταγμένη*) και καλείται *θεμελιώδης λύση*[9] τής (5.17). Όταν $\ell \equiv 0 (\mathrm{mod}\, 2)$, η (5.18) δεν διαθέτει ακέραιες λύσεις, ενώ όταν $\ell \equiv 1 (\mathrm{mod}\, 2)$, το διατεταγμένο ζεύγος

$$\boxed{(x_1', y_1') := (p_{\ell-1}, q_{\ell-1})}$$

είναι το στοιχείο τού $\Lambda_{-1}(m)$ με την *ελάχιστη δυνατή θετική τετμημένη* (άρα και με την ελάχιστη θετική *τεταγμένη*) και καλείται *θεμελιώδης λύση* τής (5.18). Μέσω των θεμελιωδών λύσεων αποκτώνται ολόκληρα τα $\Lambda_{+1}(m)$ και $\Lambda_{-1}(m)$ (και, κατ' επέκταση, και η ομάδα (5.19)), καθώς ισχύουν οι ισότητες

$$\Lambda_{+1}(m) = \left\{ (x_n, y_n) \,\middle|\, n \in \mathbb{Z} \text{ και } x_n + y_n\sqrt{m} = \pm(x_1 + y_1\sqrt{m})^n \right\}$$

και[10]

$$\Lambda_{-1}(m) = \begin{cases} \left\{ (\varepsilon_1 x_n', \varepsilon_2 y_n') \,\middle|\, \begin{array}{l} \varepsilon_1, \varepsilon_2 \in \{\pm 1\}, n \in \mathbb{Z} \text{ και} \\ x_n' + y_n'\sqrt{m} = (x_1' + y_1'\sqrt{m})^{2n-1} \end{array} \right\}, & \text{όταν } \ell \equiv 1 (\mathrm{mod}\, 2), \\ \varnothing, & \text{όταν } \ell \equiv 0 (\mathrm{mod}\, 2). \end{cases}$$

[8] Βλ., π.χ., Δ. Πουλάκη: *Θεωρία Αριθμών*, εκδόσεις Ζήτη, Θεσσαλονίκη, 1997, κεφ. 8 και 9.

[9] Προφανώς, $(x_1 + y_1\sqrt{m})^{-n} = (x_1 - y_1\sqrt{m})^n, \forall n \in \mathbb{Z}$.

[10] Βλ. T. Nagell: *Introduction to Number Theory*, Wiley, 1951, σελ. 201-202.

Κάποιες κατά τι πρακτικότερες εκφράσεις είναι οι

$$\Lambda_{+1}(m) = \begin{cases} \{(\pm 1, 0)\} \cup \left\{ (\varepsilon_1 p_{j\ell-1}, \varepsilon_2 q_{j\ell-1}) \,\middle|\, \begin{array}{c} j \in \mathbb{N} \text{ και} \\ \varepsilon_1, \varepsilon_2 \in \{\pm 1\} \end{array} \right\}, & \text{όταν } \ell \equiv 0 (\mathrm{mod}\, 2), \\ \{(\pm 1, 0)\} \cup \left\{ (\varepsilon_1 p_{2j\ell-1}, \varepsilon_2 q_{2j\ell-1}) \,\middle|\, \begin{array}{c} j \in \mathbb{N} \text{ και} \\ \varepsilon_1, \varepsilon_2 \in \{\pm 1\} \end{array} \right\}, & \text{όταν } \ell \equiv 1 (\mathrm{mod}\, 2). \end{cases}$$

και

$$\Lambda_{-1}(m) = \begin{cases} \left\{ (\varepsilon_1 p_{(2j-1)\ell-1}, \varepsilon_2 q_{(2j-1)\ell-1}) \,\middle|\, \begin{array}{c} j \in \mathbb{N} \text{ και} \\ \varepsilon_1, \varepsilon_2 \in \{\pm 1\} \end{array} \right\}, & \text{όταν } \ell \equiv 1 (\mathrm{mod}\, 2), \\ \varnothing, & \text{όταν } \ell \equiv 0 (\mathrm{mod}\, 2). \end{cases}$$

Ιδιαιτέρως, όταν $\ell \equiv 0 (\mathrm{mod}\, 2)$,

$$\boxed{\mathbb{Z}[\sqrt{m}]^\times = \{\pm (x_1 + y_1\sqrt{m})^n \mid n \in \mathbb{Z}\},}$$

ενώ όταν $\ell \equiv 1 (\mathrm{mod}\, 2)$ λαμβάνουμε

$$x_1 + y_1\sqrt{m} = (x_1' + y_1'\sqrt{m})^2,$$

ήτοι $x_1 = (x_1')^2 + m(y_1')^2$ και $y_1 = 2x_1'y_1'$, και

$$\boxed{\mathbb{Z}[\sqrt{m}]^\times = \{\pm (x_1' + y_1'\sqrt{m})^n \mid n \in \mathbb{Z}\}.}$$

5.2.42 Παραδείγματα. (i) Όταν $m = 2$, έχουμε $a_0 = 1$, $\ell = 1$, $\sqrt{2} = [1; \overline{2}]$,

$$(x_1', y_1') = (p_0, q_0) = (a_0, 1) = (1, 1),$$

οπότε

$$\boxed{\mathbb{Z}[\sqrt{2}]^\times = \left\{\pm (1 + \sqrt{2})^n \mid n \in \mathbb{Z}\right\}.}$$

(ii) Όταν $m = 3$, έχουμε $a_0 = 1$, $\ell = 2$, $\sqrt{3} = [1; \overline{1, 2}]$, $\Lambda_{-1}(3) = \varnothing$,

$$(x_1, y_1) = (p_1, q_1) = (a_0a_1 + 1, a_1) = (2, 1),$$

και, ως εκ τούτου,

$$\boxed{\mathbb{Z}[\sqrt{3}]^\times = \left\{\pm (2 + \sqrt{3})^n \mid n \in \mathbb{Z}\right\}.}$$

(iii) Οι υπολογισμοί των ομάδων $\mathbb{Z}[\sqrt{m}]^\times$ για τους 16 αρχικούς θετικούς ακεραίους m που στερούνται τετραγώνων διευκολύνονται εάν κανείς χρησιμοποιήσει τον κά-

τωθι κατάλογο:

m	a_0	ℓ	x_1	y_1
2	1	1	3	2
3	1	2	2	1
5	2	1	9	4
6	2	2	5	2
7	2	4	8	3
10	3	1	19	6
11	3	2	10	3
13	3	4	649	180

m	a_0	ℓ	x_1	y_1
14	3	4	15	4
15	3	2	4	1
17	4	1	33	8
19	4	6	170	39
21	4	6	55	12
22	4	6	197	42
23	4	4	24	5
26	5	1	51	10

5.2.43 Πρόταση. *Για την τετραγωνική αριθμητική περιοχή* $\mathbb{Z}[\sqrt{-5}]$ *ισχύουν τα εξής*:

(i) $\text{ΜΚΔ}_{\mathbb{Z}[\sqrt{-5}]}(6, 2\left(1+\sqrt{-5}\right)) = \varnothing$.

(ii) $\text{ΕΚΠ}_{\mathbb{Z}[\sqrt{-5}]}(2, 1+\sqrt{-5}) = \varnothing$.

(iii) *Η* $\mathbb{Z}[\sqrt{-5}]$ *δεν είναι περιοχή μεγ.κ.δ.*

ΑΠΟΔΕΙΞΗ. (i) Ας υποθέσουμε ότι για τα στοιχεία $6 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$ και $2\left(1+\sqrt{-5}\right)$ διαθέτουν κάποιον μέγιστο κοινό διαιρέτη, ας τον πούμε d. Βάσει τής προτάσεως 5.1.3 και τού (iii) τής προτάσεως 5.2.39,

$$\left.\begin{aligned} d \mid 6 \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(6) = 36 \\ d \mid 2\left(1+\sqrt{-5}\right) \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(2\left(1+\sqrt{-5}\right)) = 24 \\ \text{μκδ}\,(24, 36) = 12 \text{ (εντός τού } \mathbb{Z}) \end{aligned}\right\} \Longrightarrow \mathbf{N}(d) \mid 12. \tag{5.20}$$

Επειδή $d \neq 0 \Longrightarrow \mathbf{N}(d) \geq 1$ (βλ. 5.2.39 (i) και (v)), έχουμε

$$\left.\begin{aligned} 2 \mid 6 \ \text{ (εντός τής } \mathbb{Z}[\sqrt{-5}]) \\ 2 \mid 2(1+\sqrt{-5}) \ \text{ (εντός τής } \mathbb{Z}[\sqrt{-5}]) \end{aligned}\right\} \Longrightarrow 2 \mid d \Longrightarrow 4 = \mathbf{N}(2) \mid \mathbf{N}(d),$$

και

$$\left.\begin{aligned} 1+\sqrt{-5} \mid 6 \ \text{ (εντός τής } \mathbb{Z}[\sqrt{-5}]) \\ 1+\sqrt{-5} \mid 2(1+\sqrt{-5}) \ \text{ (εντός τής } \mathbb{Z}[\sqrt{-5}]) \end{aligned}\right\} \Longrightarrow 6 = \mathbf{N}(1+\sqrt{-5}) \mid \mathbf{N}(d),$$

έχουμε

$$\left.\begin{aligned} 4 \mid \mathbf{N}(d) \\ 6 \mid \mathbf{N}(d) \\ \text{εκπ}\,(4, 6) = 12 \text{ (εντός τού } \mathbb{Z}) \end{aligned}\right\} \Longrightarrow 12 \mid \mathbf{N}(d) \tag{5.21}$$

(βλ. πρόταση 5.1.5), οπότε οι σχέσεις διαιρετότητας (5.20) και (5.21) μας πληροφορούν ότι $\mathbf{N}(d) = 12$. Επιπροσθέτως, επειδή

$$1+\sqrt{-5} \mid d \Longrightarrow \exists a, b \in \mathbb{Z} : d = (1+\sqrt{-5})(a+b\sqrt{-5}),$$

έχουμε

$$\left.\begin{array}{r} 12 = \mathbf{N}(d) = 6 \cdot \mathbf{N}\left(a + b\sqrt{-5}\right) \\ \mathbf{N}\left(a + b\sqrt{-5}\right) = a^2 + 5b^2 \geq 0 \end{array}\right\} \Longrightarrow a^2 + 5b^2 = 2.$$

Η περίπτωση να ισχύει $b \neq 0$ *αποκλείεται*, διότι τότε θα είχαμε $a^2 + 5b^2 \geq 5$. Άρα κατ' ανάγκην $b = 0$. Όμως και η εξίσωση $a^2 = 2$ *δεν* διαθέτει ακέραιες λύσεις. Ως εκ τούτου, $\text{ΜΚΔ}_{\mathbb{Z}[\sqrt{-5}]}(6, 2\left(1 + \sqrt{-5}\right)) = \varnothing$.

(ii) Ας υποθέσουμε ότι τα στοιχεία 2 και $1+\sqrt{-5}$ διαθέτουν κάποιο ελάχιστο κοινό πολλαπλάσιο t. Βάσει τής προτάσεως 5.1.5 και τού (iii) τής προτάσεως 5.2.39,

$$\left.\begin{array}{r} 2 \mid t \Rightarrow \mathbf{N}(2) = 4 \mid \mathbf{N}(t) \\ 1 + \sqrt{-5} \mid t \Rightarrow \mathbf{N}(1 + \sqrt{-5}) = 6 \mid \mathbf{N}(t) \\ \text{εκπ}\,(4, 6) = 12 \text{ (εντός τού } \mathbb{Z}) \end{array}\right\} \Longrightarrow 12 \mid \mathbf{N}(t). \tag{5.22}$$

Επειδή $t \neq 0 \Longrightarrow \mathbf{N}(t) \geq 1$ (βλ. 5.2.39 (i) και (v)) και

$$t \mid 2(1 + \sqrt{-5}) \ \text{ (εντός τής } \mathbb{Z}[\sqrt{-5}]) \Longrightarrow \mathbf{N}(t) \mid 24, \tag{5.23}$$

οι σχέσεις διαιρετότητας (5.22) και (5.23) μας πληροφορούν ότι $\mathbf{N}(t) \in \{12, 24\}$. Εάν $t = x + y\sqrt{-5}$, $x, y \in \mathbb{Z}$, τότε

$$\text{είτε } \ x^2 + 5y^2 = 12 \ \text{ είτε } \ x^2 + 5y^2 = 24.$$

Στην πρώτη περίπτωση πρέπει να ισχύει: $|y| \leq 1$ (διότι για $|y| \geq 2$ έχουμε προφανώς $x^2 + 5y^2 \geq 20$), οπότε $y \in \{0, \pm 1\}$. Για $y = 0$, η εξίσωση $x^2 = 12$ *δεν* διαθέτει ακέραιες λύσεις. Αλλά και για $y = \pm 1$, η εξίσωση $x^2 = 7$ *δεν* διαθέτει ακέραιες λύσεις. Άρα η πρώτη περίπτωση *αποκλείεται*. Στη δεύτερη περίπτωση πρέπει να ισχύει: $|y| \leq 2$ (διότι για $|y| \geq 3$ έχουμε $x^2 + 5y^2 \geq 45$) και $|x| \leq 4$ (διότι για $|x| \geq 5$ έχουμε $x^2 + 5y^2 \geq 25$). Από τον πίνακα όλων των δυνατών τιμών $(x, y) \neq (0, 0)$:

$\lvert x\rvert$	$\lvert y\rvert$	$x^2 + 5y^2$
0	1	5
0	2	20
1	0	1
1	1	6
1	2	21
2	0	4
2	1	9

$\lvert x\rvert$	$\lvert y\rvert$	$x^2 + 5y^2$
2	2	$\boxed{24}$
3	0	9
3	1	14
3	2	29
4	0	16
4	1	21
4	2	36

διαπιστώνουμε ότι οι μόνες ακέραιες λύσεις τής $x^2 + 5y^2 = 24$ είναι οι $x = \pm 2$ και $y = \pm 2$. Επομένως,

$$t \in \{\pm 2(1 + \sqrt{-5}), \pm 2(1 - \sqrt{-5})\}.$$

Επειδή τώρα το στοιχείο $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ είναι κοινό πολλαπλάσιο των 2 και $1+\sqrt{-5}$ (εντός τής $\mathbb{Z}[\sqrt{-5}]$), πρέπει $t \mid 6$, ήτοι να υπάρχουν $u, v \in \mathbb{Z}$ με

$$6 \in \left\{\pm 2(1+\sqrt{-5})(u+v\sqrt{-5}), \pm 2(1-\sqrt{-5})(u+v\sqrt{-5})\right\},$$

ή, ισοδυνάμως,

$$\pm 3 \in \left\{(u-5v)+(u+v)\sqrt{-5}, (u+5v)+(u-v)\sqrt{-5}\right\}$$

πράγμα αδύνατο, καθότι οι $\pm 3 = \mp 6v$ δεν επιδέχονται ακέραιες λύσεις. Άρα *και* η δεύτερη περίπτωση *αποκλείεται*. Ως εκ τούτου, $\text{ΕΚΠ}_{\mathbb{Z}[\sqrt{-5}]}(2, 1+\sqrt{-5}) = \varnothing$.
(iii) Τούτο έπεται άμεσα από το (i) ή -εναλλακτικώς- από το (ii). □

5.3 ΠΡΩΤΑ ΚΑΙ ΑΝΑΓΩΓΑ ΣΤΟΙΧΕΙΑ

5.3.1 Ορισμός. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Ένα στοιχείο $p \in R$ καλείται **πρώτο στοιχείο** τού R όταν $p \in R \setminus (R^\times \cup \{0_R\})$ και, επιπροσθέτως, για οιαδήποτε $a, b \in R$ ισχύει η συνεπαγωγή:

$$[p \mid ab \Longrightarrow \text{είτε } p \mid a \text{ είτε } p \mid b].$$

5.3.2 Ορισμός. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Ένα στοιχείο $q \in R$ καλείται **ανάγωγο στοιχείο** τού R όταν $q \in R \setminus (R^\times \cup \{0_R\})$ και, επιπροσθέτως, για οιαδήποτε $a, b \in R$ ισχύει η συνεπαγωγή:

$$[q = ab \Longrightarrow \text{είτε } a \in R^\times \text{ είτε } b \in R^\times].$$

5.3.3 Παραδείγματα. (i) Στον δακτύλιο $\mathbb{Z}$ των ακεραίων αριθμών ένα στοιχείο είναι πρώτο εάν και μόνο εάν είναι ανάγωγο, ήτοι τής μορφής $\pm p$, όπου p κάποιος πρώτος αριθμός.
(ii) Στον δακτύλιο $\mathbb{Z}_6$ (που είναι Δ.Κ.Ι. αλλά όχι Π.Κ.Ι.) το στοιχείο $[2]_6$ είναι πρώτο. Πράγματι· τα μόνα γινόμενα στοιχείων τού $\mathbb{Z}_6$ τα οποία διαιρεί το $[2]_6$ είναι τα

$$[1]_6\,[2]_6\,, [1]_6\,[4]_6\,, [2]_6\,[3]_6\,, [2]_6\,[4]_6\,, [2]_6\,[5]_6\,, [3]_6\,[4]_6\,, [4]_6\,[5]_6\,.$$

Αρκεί λοιπόν να παρατηρήσουμε ότι το $[2]_6$ διαιρεί τουλάχιστον έναν εκ των παραγόντων αυτών των γινομένων. Από την άλλη μεριά, το $[2]_6$ *δεν είναι* ανάγωγο στοιχείο τού $\mathbb{Z}_6$, αφού

$$[2]_6 = [4]_6\,[2]_6\,, \quad [4]_6 \notin \mathbb{Z}_6^\times, \quad [2]_6 \notin \mathbb{Z}_6^\times \,(= \{[1]_6\,, [5]_6\}).$$

(iii) Στην υποπεριοχή $R = \left\{\frac{a}{2^n} \in \mathbb{Q} \;\middle|\; a \in \mathbb{Z},\ n \in \mathbb{N}_0\right\}$ τού σώματος των ρητών αριθμών (βλ. άσκηση **1-31**) το στοιχείο $6 = \frac{6}{2^0}$ είναι ανάγωγο. Πράγματι· εάν το 6 γράφεται ως γινόμενο $6 = \frac{a}{2^n}\frac{b}{2^m}$, όπου $a, b \in \mathbb{Z},\ n, m \in \mathbb{N}_0$, τότε

$$ab = 2^{n+m+1}\cdot 3, \text{ με } n+m+1 \geq 1,$$

απ' όπου έπεται ότι $3 \mid ab \Longrightarrow$ είτε $3 \mid a$ είτε $3 \mid b$ (εντός τού $\mathbb{Z}$!). Εάν $3 \mid a$, τότε $a = 3r$ για κάποιον $r \in \mathbb{Z}$, οπότε

$$rb = 2^{n+m+1} \Longrightarrow b = 2^{\mu}, \text{ για κάποιον } \mu \in \mathbb{N}_0,\ \mu \leq n+m+1.$$

Κατά συνέπειαν, $\frac{b}{2^m} = 2^{\mu-m} \in R^{\times} = \{\pm 2^{\nu} \mid \nu \in \mathbb{Z}\}$. Εάν $3 \mid b$, τότε -κατ' αναλογίαν- $\frac{a}{2^n} \in R^{\times}$.

(iv) Στον δακτύλιο $\mathbb{Z}[i]$ των ακεραίων τού Gauss (που είναι ακεραία περιοχή) ένα στοιχείο είναι πρώτο εάν και μόνο εάν είναι ανάγωγο (πρβλ. 5.3.4 (iv)). Μάλιστα, το θεώρημα 5.7.4 περιγράφει λεπτομερώς τη μορφή όλων των αναγώγων στοιχείων τού $\mathbb{Z}[i]$. Από την άλλη μεριά, στην ακεραία περιοχή $\mathbb{Z}[\sqrt{-3}]$ υπάρχουν ανάγωγα στοιχεία (όπως, π.χ., το 2) που δεν είναι πρώτα (βλ. τα (i) και (ii) τής προτάσεως 5.3.8).

5.3.4 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε ισχύουν τα ακόλουθα*:

(i) *Ένα $p \in R \setminus (R^{\times} \cup \{0_R\})$ είναι πρώτο στοιχείο τής R εάν και μόνον εάν το κύριο ιδεώδες $\langle p \rangle$ είναι ένα μη τετριμμένο πρώτο ιδεώδες τής R.*

(ii) *Ένα $q \in R \setminus (R^{\times} \cup \{0_R\})$ είναι ανάγωγο στοιχείο τής R εάν και μόνον εάν το κύριο ιδεώδες $\langle q \rangle$ είναι ένα μεγιστικό στοιχείο τού συνόλου όλων των γνησίων μη τετριμμένων κυρίων ιδεωδών τής R (ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό).*

(iii) *Κάθε πρώτο στοιχείο τής R είναι ανάγωγο*[11].

(iv) *Εάν η R είναι Π.Κ.Ι., τότε ένα $p \in R \setminus (R^{\times} \cup \{0_R\})$ είναι πρώτο στοιχείο τής R εάν και μόνον εάν είναι ανάγωγο στοιχείο τής R.*

(v) *Εάν το p είναι ένα πρώτο στοιχείο τής R και $p \underset{\text{συν.}}{\sim} p'$, για κάποιο $p' \in R$, τότε και το p' είναι ένα πρώτο στοιχείο τής R.*

(vi) *Εάν το q είναι ένα ανάγωγο στοιχείο τής R και $q \underset{\text{συν.}}{\sim} q'$, για κάποιο $q' \in R$, τότε και το q' είναι ένα ανάγωγο στοιχείο τής R.*

(vii) *Οι μόνοι διαιρέτες ενός αναγώγου στοιχείου q τής R είναι τα συντροφικά του στοιχεία και τα αντιστρέψιμα στοιχεία τής R, ήτοι οι «μη γνήσιοι» διαιρέτες τού q* (βλ. 5.2.8).

(viii) *Ένα $q \in R \setminus (R^{\times} \cup \{0_R\})$ είναι ανάγωγο στοιχείο τής R εάν και μόνον εάν δεν διαθέτει «γνήσιους» διαιρέτες.*

ΑΠΟΔΕΙΞΗ. (i) Έστω $p \in R \setminus (R^{\times} \cup \{0_R\})$ ένα πρώτο στοιχείο τής R. Επειδή το p είναι μη μηδενικό και μη αντιστρέψιμο, έχουμε $\{0_R\} \subsetneqq \langle p \rangle \subsetneqq R$. Υποθέτοντας ότι $a, b \in R$ με $ab \in \langle p \rangle$, έχουμε $p \mid ab$, οπότε είτε $p \mid a$ είτε $p \mid b$, δηλαδή είτε $a \in \langle p \rangle$ είτε $b \in \langle p \rangle$. Άρα το $\langle p \rangle$ είναι ένα μη τετριμμένο πρώτο ιδεώδες τής R. Και αντιστρόφως· υποθέτοντας ότι το το $\langle p \rangle$ είναι ένα μη τετριμμένο πρώτο ιδεώδες τής

[11] Όπως είδαμε στο παράδειγμα 5.3.3 (ii), τούτο δεν είναι πάντοτε αληθές για μεταθετικούς δακτυλίους R με μοναδιαίο στοιχείο οι οποίοι *δεν είναι* ακέραιες περιοχές!

R, το στοιχείο p που το παράγει είναι μη μηδενικό και μη αντιστρέψιμο (βλ. 2.1.6), και εάν $a, b \in R$ με $p \mid ab$, τότε

$$ab \in \langle p\rangle \Longrightarrow \text{είτε } \ a \in \langle p\rangle \ \text{ είτε } b \in \langle p\rangle \Longrightarrow \text{είτε } \ p \mid a \ \text{ είτε } \ p \mid b,$$

οπότε το p είναι ένα πρώτο στοιχείο τής ακεραίας περιοχής R.

(ii) Έστω q ένα ανάγωγο στοιχείο τής R. Προφανώς, $\{0_R\} \subsetneqq \langle q\rangle \subsetneqq R$. Έστω $\langle a\rangle$ τυχόν μη τετριμμένο γνήσιο κύριο ιδεώδες τής R με $\langle q\rangle \subseteq \langle a\rangle$. Τότε $q = ar$ για κάποιο $r \in R$. Επομένως, είτε $a \in R^\times$ είτε $r \in R^\times$. Η πρώτη περίπτωση αποκλείεται (καθότι υπετέθη πως το $\langle a\rangle$ είναι *γνήσιο* ιδεώδες τής R). Άρα $r \in R^\times$, οπότε

$$q \underset{\text{συν.}}{\sim} a \Longleftrightarrow \langle q\rangle = \langle a\rangle \Longrightarrow \left\{ \begin{array}{c} \text{Το } \langle q\rangle \text{ είναι ένα μεγιστικό στοιχείο} \\ \text{τού συνόλου όλων των μη τετριμμένων} \\ \text{γνησίων κυρίων ιδεωδών τής } R. \end{array} \right\}.$$

Και αντιστρόφως· εάν υποθέσουμε ότι το κύριο ιδεώδες $\langle q\rangle$ είναι ένα μεγιστικό στοιχείο τού συνόλου όλων των μη τετριμμένων γνησίων κυρίων ιδεωδών τής R (ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό), τότε $\{0_R\} \subsetneqq \langle q\rangle \subsetneqq R$, οπότε το q δεν είναι ούτε $= 0_R$ ούτε αντιστρέψιμο. Επιπροσθέτως, εάν $a, b \in R$ με $q = ab$, έχουμε

$$\langle q\rangle \subseteq \langle a\rangle \Longrightarrow \text{είτε } \ \langle q\rangle = \langle a\rangle \ \text{ είτε } \ \langle a\rangle = R.$$

Εάν ισχύει η ισότητα $\langle q\rangle = \langle a\rangle$, τότε $a = qc$ για κάποιο $c \in R$, οπότε

$$q = ab = qbc \underset{\text{(βλ. 1.2.5)}}{\Longrightarrow} bc = 1 \Longrightarrow b \in R^\times.$$

Εάν, από την άλλη μεριά, ισχύει η ισότητα $\langle a\rangle = R$, τότε $a \in R^\times$. Κατά συνέπειαν, το q είναι ένα ανάγωγο στοιχείο τής R.

(iii) Έστω p ένα πρώτο στοιχείο τής R. Εάν $a, b \in R$ με $p = ab$, έχουμε

$$\text{είτε } \ p \mid a \ \text{ είτε } \ p \mid b \Longrightarrow \text{είτε } \left\{ \begin{array}{c} a = pr \\ \text{για κάποιο } r \in R \end{array} \right\} \ \text{ είτε } \ \left\{ \begin{array}{c} b = ps \\ \text{για κάποιο } s \in R \end{array} \right\}.$$

Επομένως, είτε $rb = 1$ είτε $sa = 1$, δηλαδή είτε $b \in R^\times$ είτε $a \in R^\times$. Άρα το p είναι ένα ανάγωγο στοιχείο τής R.

(iv) Λόγω τού (iii), αρκεί να αποδειχθεί ότι κάθε ανάγωγο στοιχείο μιας Π.Κ.Ι. R είναι πρώτο. Εάν λοιπόν το q είναι ανάγωγο, τότε $\{0_R\} \subsetneqq \langle q\rangle \subsetneqq R$ και (κατά το (ii)) το $\langle q\rangle$ είναι ένα μεγιστικό στοιχείο τού συνόλου όλων των μη τετριμμένων γνησίων κυρίων ιδεωδών τής R (ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό). Επειδή η ακεραία περιοχή R είναι Π.Κ.Ι., το $\langle q\rangle$ είναι κατ' ανάγκην μεγιστικό ιδεώδες τής R. Όμως κάθε μεγιστικό ιδεώδες τής R είναι πρώτο ιδεώδες (βλ. θεώρημα 2.5.22). Άρα το $\langle q\rangle$ είναι πρώτο ιδεώδες και (βάσει τού (i)) το q είναι πρώτο στοιχείο τής R.

(v) Εάν το p είναι ένα πρώτο στοιχείο τής R και $p \underset{\text{συν.}}{\sim} p'$, τότε $p' = up$ για κάποιο $u \in R^\times$. Υποθέτοντας ότι $a, b \in R$ με $p' \mid ab$, έχουμε

$$\left.\begin{matrix} p \mid p' \\ p' \mid ab \end{matrix}\right\} \Longrightarrow p \mid ab \Longrightarrow \text{είτε } \ p \mid a \ \text{ είτε } \ p \mid b.$$

Ως εκ τούτου, είτε $a = pr = u^{-1}p'r$ για κάποιο $r \in R$ είτε $b = ps = u^{-1}p's$ για κάποιο $s \in R$, απ' όπου συμπεραίνουμε ότι είτε $p' \mid a$ είτε $p' \mid b$. Κατά συνέπειαν, *και* το p'είναι ένα πρώτο στοιχείο τής ακεραίας περιοχής R.

(vi) Εάν το q είναι ένα ανάγωγο στοιχείο τής R και $q \underset{\text{συν.}}{\sim} q'$, τότε $q = uq'$ για κάποιο $u \in R^\times$. Υποθέτοντας ότι $a, b \in R$ με $q' = ab$, έχουμε

$$q = uab \Longrightarrow \text{είτε } \ ua \in R^\times \ \text{ είτε } \ b \in R^\times \Longrightarrow \text{είτε } \ a \in R^\times \ \text{ είτε } \ b \in R^\times,$$

οπότε *και* το q' είναι ένα ανάγωγο στοιχείο τής ακεραίας περιοχής R.

(vii) Έστω τυχόν $a \in R$ που είναι διαιρέτης τού q. Τότε $\langle q \rangle \subseteq \langle a \rangle$. Επειδή (κατά το (ii)) το κύριο ιδεώδες $\langle q \rangle$ είναι ένα μεγιστικό στοιχείο τού συνόλου όλων των μη τετριμμένων γνησίων κυρίων ιδεωδών τής R (ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό), συμπεραίνουμε ότι $\langle q \rangle = \langle a \rangle$. Τούτο σημαίνει ότι είτε τα q και a είναι συντροφικά (βλ. 5.2.4 (ii)) είτε $\langle q \rangle = \langle a \rangle = R$, οπότε το a είναι αντιστρέψιμο.

(viii) Εάν το $q \in R \setminus (R^\times \cup \{0_R\})$ είναι ανάγωγο στοιχείο τής ακεραίας περιοχής R, τότε αυτό δεν διαθέτει γνήσιους διαιρέτες βάσει τού (vii). Εάν, αντιστρόφως, ένα στοιχείο $q \in R \setminus (R^\times \cup \{0_R\})$ δεν διαθέτει γνήσιους διαιρέτες και υπάρχουν $a, b \in R$, τέτοια ώστε να ισχύει η ισότητα $q = ab$, τότε, επειδή $a \mid q$ και $b \mid q$, έχουμε

$$\Big(\text{είτε } \ a \in R^\times \ \text{ είτε } \ q \underset{\text{συν.}}{\sim} a\Big) \ \text{ και } \ \Big(\text{είτε } \ b \in R^\times \ \text{ είτε } \ q \underset{\text{συν.}}{\sim} b\Big).$$

Υποθέτοντας ότι $q \underset{\text{συν.}}{\sim} a$ και $q \underset{\text{συν.}}{\sim} b$, συμπεραίνουμε ότι

$$q^2 \underset{\text{συν.}}{\sim} ab = q \Longrightarrow \exists x \in R^\times : q^2 = qx.$$

(βλ. 5.2.5 και 5.2.7). Επειδή ο θεωρούμενος δακτύλιος R είναι εξ υποθέσεως ακεραία περιοχή (βλ. 1.2.5), η ως άνω ισότητα ισοδυναμεί με την $q = x \in R^\times$, κάτι το οποίο είναι άτοπο. Άρα είτε $a \in R^\times$ είτε $b \in R^\times$ και, ως εκ τούτου, το q είναι ανάγωγο στοιχείο τής R. □

5.3.5 Πόρισμα. *Έστω R μια Π.Κ.Ι. Τότε ισχύουν τα ακόλουθα*:

(i) *Το p είναι πρώτο στοιχείο τής R εάν και μόνον εάν το κύριο ιδεώδες $\langle p \rangle$ είναι ένα μη τετριμμένο πρώτο ιδεώδες τής R.*

(ii) *Το q είναι ανάγωγο στοιχείο τής R εάν και μόνον εάν το κύριο ιδεώδες $\langle q \rangle$ είναι ένα μεγιστικό ιδεώδες τής R.*

(iii) *Ένα στοιχείο τής R είναι πρώτο εάν και μόνον εάν είναι ανάγωγο.*

(iv) *Ένα μη τετριμμένο ιδεώδες τής R είναι πρώτο εάν και μόνον εάν είναι μεγιστικό.*

ΑΠΟΔΕΙΞΗ. Είναι προφανές ότι τα (i), (ii) και (iv) έπονται άμεσα από την προηγηθείσα πρόταση 5.3.4. (Το (iv) είχε αποδειχθεί και ανεξαρτήτως αυτής στην πρόταση 4.2.15). Εξάλλου, επειδή κάθε ιδεώδες τής R είναι κύριο, το (iii) έπεται από το ότι κάθε μεγιστικό ιδεώδες τής R είναι μεγιστικό στοιχείο τού συνόλου των γνησίων ιδεωδών της και το (ii) τής 5.3.4. □

5.3.6 Πρόταση. *Ένα στοιχείο μιας περιοχής R με μ.κ.δ. είναι πρώτο εάν και μόνον εάν είναι ανάγωγο.*

ΑΠΟΔΕΙΞΗ. Λόγω τού (iii) τής προτάσεως 5.3.4 αρκεί να αποδείξουμε ότι κάθε ανάγωγο στοιχείο τής R είναι πρώτο. Έστω $q \in R \setminus (R^\times \cup \{0_R\})$ τυχόν ανάγωγο στοιχείο τής R. Ας υποθέσουμε ότι υπάρχουν $a, b \in R$, τέτοια ώστε $q \mid ab$. Εάν $q \nmid a$ και $d \in \mathrm{MK}\Delta_R(q, a)$, τότε, σύμφωνα με το (ii) τής προτάσεως 5.2.35, $d \underset{\text{συν.}}{\not\sim} q$. Ωστόσο, $d \mid q$, οπότε υπάρχει $q' \in R$, τέτοιο ώστε να ισχύει η ισότητα $q = dq'$. Επειδή το q είναι ανάγωγο στοιχείο, έχουμε κατ' ανάγκην είτε $d \in R^\times$ είτε $q' \in R^\times$. Όμως $d \underset{\text{συν.}}{\not\sim} q \Longrightarrow q' \notin R^\times$. Κατά συνέπειαν, $d \in R^\times \Longrightarrow d \underset{\text{συν.}}{\sim} 1_R$, οπότε τα q και a είναι σχετικώς πρώτα. Από το (i) τής προτάσεως 5.2.37 συμπεραίνουμε ότι $q \mid b$. (Παρομοίως αποδεικνύεται, ύστερα από εναλλαγή των ρόλων των a και b, ότι εάν $q \nmid b$, τότε $q \mid a$.) Άρα το q είναι όντως πρώτο στοιχείο τής R. □

5.3.7 Παράδειγμα. Όπως έχουμε δείξει στα εδάφια 4.2.13 και 5.2.43, η ακεραία περιοχή $\mathbb{Z}[\sqrt{-5}]$ δεν είναι ούτε Π.Κ.Ι. ούτε καν περιοχή με μ.κ.δ. Εναλλακτικώς, αυτό το συμπέρασμα μπορεί (λόγω τής 5.3.6) να εξαχθεί και απευθείας παρατηρώντας οτι το 2 είναι ανάγωγο, χωρίς όμως να είναι και πρώτο στοιχείο της. Όπως μας δείχνει η επόμενη πρόταση, η ιδιότητα αυτή ισχύει γενικότερα και για τετραγωνικές αριθμητικές περιοχές αντιστοιχιζόμενες σε *απείρου πλήθους* ακεραίους m.

5.3.8 Πρόταση. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Τότε ισχύουν τα ακόλουθα*:

(i) *Το 2 δεν είναι πρώτο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$ (παρότι είναι πρώτο στοιχείο εντός τού $\mathbb{Z}$!)*

(ii) *Εάν για τον m ισχύει είτε $m \equiv 1 (\mathrm{mod}\, 4)$ είτε $m \leq -3$, τότε το 2 είναι ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$.*

(iii) *Εάν για τον m ισχύει είτε $m \equiv 1 (\mathrm{mod}\, 4)$ είτε $m \leq -3$, τότε η $\mathbb{Z}[\sqrt{m}]$ δεν είναι ούτε Π.Κ.Ι. ούτε περιοχή με μκδ.*

ΑΠΟΔΕΙΞΗ. Επειδή $\mathbf{N}(2) = 4 \notin \{0, \pm 1\}$, έχουμε $2 \in \mathbb{Z}[\sqrt{m}] \setminus (\mathbb{Z}[\sqrt{m}]^\times \cup \{0\})$ (επί τη βάσει των (i) και (vi) τής προτάσεως 5.2.39), όπου $\mathbf{N}$ η αριθμητική στάθμη τού $\mathbb{Q}(\sqrt{m})$ (βλ. 5.2.38).

(i) Επειδή το γινόμενο $m(m-1) \in \mathbb{Z}$ είναι πάντοτε ένας άρτιος ακέραιος, έχουμε

$$2 \mid m(m-1) = \left(m + \sqrt{m}\right)\left(m - \sqrt{m}\right).$$

Εάν το 2 ήταν πρώτο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$, θα έπρεπε

$$\text{είτε } 2 \mid m+\sqrt{m} \text{ είτε } 2 \mid m-\sqrt{m},$$

απ' όπου θα καταλήγαμε σε κάτι το οποίο είναι άτοπο, αφού εξισώσεις τής μορφής

$$m \pm \sqrt{m} = 2\left(x + y\sqrt{m}\right),\ x, y \in \mathbb{Z},$$

δεν επιδέχονται ακέραιες λύσεις ($2x = m$, $2y = \pm 1$). Άρα το 2 δεν είναι πρώτο στοιχείο τής ακεραίας περιοχής $\mathbb{Z}[\sqrt{m}]$.

(ii) Ας υποθέσουμε ότι το $a + b\sqrt{m}$, $a, b \in \mathbb{Z}$, είναι ένας *γνήσιος* διαιρέτης τού 2 εντός τής $\mathbb{Z}[\sqrt{m}]$. Από τα (iii), (vi) και (vii) τής προτάσεως 5.2.39 έπεται ότι

$$\left.\begin{array}{r} |\mathbf{N}\left(a+b\sqrt{m}\right)| \mid |\mathbf{N}(2)| = 4 \\ \mathbf{N}\left(a+b\sqrt{m}\right) \neq \pm 1 \\ |\mathbf{N}\left(a+b\sqrt{m}\right)| \neq |\mathbf{N}(2)| = 4 \end{array}\right\} \Longrightarrow \left|\mathbf{N}\left(a+b\sqrt{m}\right)\right| = 2,$$

οπότε

$$\pm\left(a^2 - mb^2\right) = 2. \tag{5.24}$$

Πρώτη περίπτωση. Εάν $m \equiv 1 (\mathrm{mod}\, 4)$, τότε $m = 4k+1$ για κάποιον $k \in \mathbb{Z}$. Η ισότητα (5.24) γράφεται ως εξής:

$$a^2 - b^2 = 2\left(2kb^2 \pm 1\right). \tag{5.25}$$

Επειδή το δεξιό μέλος τής (5.25) είναι ένας άρτιος ακέραιος αριθμός, τα a και b οφείλουν να είναι *αμφότερα* είτε άρτιοι είτε περιττοί ακέραιοι. Εάν $a = 2\mu$ και $b = 2\nu$ για κάποιους $\mu, \nu \in \mathbb{Z}$, τότε

$$a^2 - b^2 = 4(\mu^2 - \nu^2) \Longrightarrow 4 \mid a^2 - b^2,$$

πράγμα αδύνατο (διότι $a^2 - b^2 \equiv 2 (\mathrm{mod}\, 4)$ βάσει τής (5.25)). Εάν, από την άλλη μεριά, $a = 2u+1$ και $b = 2v+1$ για κάποιους $u, v \in \mathbb{Z}$, τότε και πάλι

$$a^2 - b^2 = 4(u^2 + u - v^2 - v) \Longrightarrow 4 \mid a^2 - b^2,$$

πράγμα που, όπως προείπαμε, είναι αδύνατο. Ως εκ τούτου, το 2 είναι ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$, αφού δεν διαθέτει γνήσιους διαιρέτες (βλ. το (viii) τής προτάσεως 5.3.4).

Δεύτερη περίπτωση. Εάν $m \leq -3$, τότε η ισότητα (5.24) γράφεται ως εξής:

$$2 = \left|a^2 - mb^2\right| = a^2 + |m|\, b^2. \tag{5.26}$$

Εάν $b = 0$, τότε η (5.26) είναι αδύνατη, αφού η $a^2 = 2$ δεν επιδέχεται ακέραιες λύσεις. Όμως η (5.26) είναι αναληθής ακόμη και όταν $b \neq 0$, επειδή

$$m \leq -3 \Longrightarrow |m| \geq 3 \Longrightarrow a^2 + |m|\, b^2 \geq 3.$$

Άρα το 2 είναι ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$, αφού δεν διαθέτει γνήσιους διαιρέτες (βλ. το (viii) τής προτάσεως 5.3.4).

(iii) Τούτο έπεται άμεσα από τα (i), (ii), το (iv) τής προτάσεως 5.3.4 και την πρόταση 5.3.6. □

5.3.9 Πρόταση. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων και έστω $z \in \mathbb{Z}[\sqrt{m}]$. Εάν $\mathbf{N}(z) \in \{\pm p\}$, όπου $\mathbf{N}$ η αριθμητική στάθμη τού $\mathbb{Q}(\sqrt{m})$* (βλ. 5.2.38) *και p κάποιος πρώτος αριθμός, τότε το z είναι ανάγωγο στοιχείο τής τετραγωνικής αριθμητικής περιοχής $\mathbb{Z}[\sqrt{m}]$.*

ΑΠΟΔΕΙΞΗ. Επειδή $\mathbf{N}(z) \notin \{0, \pm 1\}$, έχουμε $z \in \mathbb{Z}[\sqrt{m}] \setminus (\mathbb{Z}[\sqrt{m}]^\times \cup \{0\})$ (βλ. ιδιότητες 5.2.39 (i) και (vi)). Εάν τα u, w είναι στοιχεία τής $\mathbb{Z}[\sqrt{m}]$, τέτοια ώστε να ισχύει η ισότητα $z = uw$, τότε

$$\mathbf{N}(z) = \mathbf{N}(uw) = \mathbf{N}(u)\,\mathbf{N}(w) \in \{\pm p\}$$

οπότε *είτε* $\mathbf{N}(u) \in \{\pm 1\}$ και $\mathbf{N}(w) \in \{\pm p\}$ *είτε* $\mathbf{N}(w) \in \{\pm 1\}$ και $\mathbf{N}(u) \in \{\pm p\}$. Αυτό σημαίνει ότι είτε $u \in \mathbb{Z}[\sqrt{m}]^\times$ είτε $w \in \mathbb{Z}[\sqrt{m}]^\times$ (βλ. 5.2.39 (ii) και (vi)). Άρα το z είναι όντως ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$. □

5.3.10 Σημείωση. Η ικανή συνθήκη η οποία δίδεται στην πρόταση 5.3.9 προκειμένου ένα $z \in \mathbb{Z}[\sqrt{m}]$ να είναι ανάγωγο στοιχείο, δεν είναι και αναγκαία. Επί παραδείγματι, βάσει τής προτάσεως 5.3.8 το 2 είναι ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{-3}]$ αλλά $\mathbf{N}(2) = 4$.

5.4 ΕΥΚΛΕΙΔΕΙΕΣ ΠΕΡΙΟΧΕΣ

5.4.1 Ορισμός. Έστω R μια ακεραία περιοχή. Η R ονομάζεται **ευκλείδεια περιοχή** όταν υπάρχει μια απεικόνιση $\boldsymbol{\delta} : R \setminus \{0_R\} \longrightarrow \mathbb{N}_0$ που ικανοποιεί τις ακόλουθες συνθήκες:

(i) Εάν $a, b \in R \setminus \{0_R\}$, τότε $\boldsymbol{\delta}(ab) \geq \boldsymbol{\delta}(a)$, και

(ii) για οιαδήποτε $a \in R$ και $b \in R \setminus \{0_R\}$ υπάρχουν $(q, r) \in R \times R$ (όχι κατ' ανάγκην μονοσημάντως ορισμένα), τέτοια ώστε να ισχύει

$$\boxed{a = qb + r, \ \text{όπου είτε } r = 0_R \ \text{ είτε } \ (r \neq 0_R \ \text{ και } \ \boldsymbol{\delta}(r) < \boldsymbol{\delta}(b))\,.} \qquad (5.27)$$

(Η απεινόνιση $\boldsymbol{\delta}$ καλείται **ευκλείδεια στάθμη** ή **ευκλείδεια εκτίμηση** τής R.)

5.4.2 Σημείωση. (i) Η συνθήκη (i) τού ορισμού 5.4.1 μπορεί να αναδιατυπωθεί ως εξής: Εάν $x, y \in R \setminus \{0_R\}$ και $x \mid y$, τότε $\boldsymbol{\delta}(y) \geq \boldsymbol{\delta}(x)$.

(ii) Οι $(q,r) \in R \times R$ στην (5.27) καλούνται **πηλίκο** και, αντιστοίχως, **υπόλοιπο** τής **διαιρέσεως τού** a **διά τού** b **ως προς την** $\boldsymbol{\delta}$ *χωρίς*, ωστόσο, να χαίρουν κατ' ανάγκην *αμφοτέρων* των ιδιοτήτων των αντιστοίχων εννοιών που συναντήσαμε εργαζόμενοι στο σύνολο των ακεραίων αριθμών. (Βλ. εδάφιο 5.4.17, καθώς και την πρόταση 5.4.18, η οποία μας παρέχει μια ικανή και αναγκαία συνθήκη για τη διασφάλιση τής *μοναδικότητάς* τους, υπό τις προϋποθέσεις τού 5.4.1 (ii), *όχι* όμως και υπό την έννοια τού θεωρήματος 5.1.1!)

(iii) Μια ευκλείδεια περιοχή R εφοδιάζεται με απείρου πλήθους *διαφορετικές* ευκλείδειες στάθμες $\boldsymbol{\delta}$ (βλ. άσκηση ??). Ως εκ τούτου, όταν εργαζόμαστε με συγκεκριμένα παραδείγματα, η αναφορά μας σε κάποια ευκλείδεια περιοχή πρέπει να συνοδεύεται από τον τύπο ορισμού τής επιλεγόμενης $\boldsymbol{\delta}$.

5.4.3 Παραδείγματα. (i) Κάθε σώμα K καθίσταται ευκλείδεια περιοχή εφοδιαζόμενο με την ευκλείδεια στάθμη

$$\boldsymbol{\delta} : K \smallsetminus \{0_K\} \longrightarrow \mathbb{N}_0, \;\; \boldsymbol{\delta}\,(a) := 1, \; \forall a \in K \smallsetminus \{0_K\},$$

διότι για οιαδήποτε $a \in K$ και $b \in K \smallsetminus \{0_K\}$ ισχύει η (5.27) για τα $q = ab^{-1}$ και $r = 0_K$.

(ii) Ο δακτύλιος $\mathbb{Z}$ των ακεραίων αριθμών είναι ευκλείδεια περιοχή όταν εφοδιάζεται με οιαδήποτε εκ των σταθμών

$$\boldsymbol{\delta}_k : \mathbb{Z} \smallsetminus \{0\} \longrightarrow \mathbb{N}_0, \;\; \boldsymbol{\delta}_k\,(a) := |a|^k, \; \forall a \in \mathbb{Z}, \; \forall k \in \mathbb{N},$$

(βλ. άσκηση ??). Ειδικότερα, η $\boldsymbol{\delta}_1$ καλείται **συνήθης ευκλείδεια στάθμη** τού $\mathbb{Z}$.

(iii) Εάν επί τού υποσυνόλου των μη μηδενικών στοιχείων τού δακτυλίου

$$\mathbb{Z}_{\langle p \rangle} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; (a,b) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\}) \text{, με μκδ}\,(a,b) = 1 \text{ και } p \nmid b \right\}$$

των p-αδικών κλασμάτων (όπου p πρώτος, βλ. άσκηση **1-16**, σελ. 35) ορίσουμε την απεικόνιση

$$\boldsymbol{\delta} : \mathbb{Z}_{\langle p \rangle} \smallsetminus \{0\} \longrightarrow \mathbb{N}_0, \;\; \boldsymbol{\delta}\left(\tfrac{a}{b}\right) := \max\left\{k \in \mathbb{N}_0 : p^k \mid a\right\},$$

(τη λεγομένη, ιδιαιτέρως, p-**αδική προσθετική εκτίμηση** τού $\mathbb{Z}_{\langle p \rangle}$), τότε, για οιαδήποτε στοιχεία $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathbb{Z}_{\langle p \rangle} \smallsetminus \{0\}$, έχουμε προφανώς

$$\left.\begin{array}{r} \boldsymbol{\delta}\left(\frac{a_1}{b_1}\frac{a_2}{b_2}\right) = \boldsymbol{\delta}\left(\frac{a_1}{b_1}\right) + \boldsymbol{\delta}\left(\frac{a_2}{b_2}\right) \\ \boldsymbol{\delta}\left(\frac{a_2}{b_2}\right) \geq 0 \end{array}\right\} \Longrightarrow \boldsymbol{\delta}\left(\frac{a_1}{b_1}\frac{a_2}{b_2}\right) \geq \boldsymbol{\delta}\left(\frac{a_1}{b_1}\right).$$

Ας υποθέσουμε ότι $\frac{a_1}{b_1} \in \mathbb{Z}_{\langle p \rangle}$, $\frac{a_2}{b_2} \in \mathbb{Z}_{\langle p \rangle} \smallsetminus \{0\}$ και ότι

$$\nu_1 := \max\left\{k \in \mathbb{N}_0 : p^k \mid a_1\right\}, \;\; \nu_2 := \max\left\{k \in \mathbb{N}_0 : p^k \mid a_2\right\}.$$

Εάν διαιρέσουμε το a_1 διά τού a_2 (εντός τού $\mathbb{Z}$), λαμβάνουμε $a_1 = a_2\pi + \rho$, όπου το ζεύγος $(\pi, \rho) \in \mathbb{Z}$ είναι μονοσημάντως ορισμένο και ισχύει $0 \leq \rho \leq |a_2|$. Γράφοντας τα a_1 και a_2 ως $a_1 = p^{\nu_1}a_1', a_2 = p^{\nu_2}a_2'$, για κατάλληλα (μονοσημάντως ορισμένα) $a_1', a_2' \in \mathbb{Z}$ με μκδ$(a_1', p) =$ μκδ$(a_2', p) = 1$, ορίζουμε στοιχεία q και r τού $\mathbb{Z}_{\langle p\rangle}$ ως ακολούθως:

$$q := \begin{cases} \frac{a_1 b_2}{a_2 b_1}, & \text{όταν } \nu_1 \geq \nu_2, \\ \frac{\pi b_2}{b_1}, & \text{όταν } \nu_1 < \nu_2, \end{cases} \qquad r := \begin{cases} 0, & \text{όταν } \nu_1 \geq \nu_2, \\ \frac{\rho}{b_1}, & \text{όταν } \nu_1 < \nu_2. \end{cases}$$

Προφανώς, *και* στις δύο περιπτώσεις, ισχύει η ισότητα

$$\frac{a_1}{b_1} = \frac{a_2}{b_2}q + r.$$

Όταν $\rho \neq 0$, τότε στη δεύτερη εξ αυτών (ήτοι όταν $\nu_1 < \nu_2$) έχουμε

$$\nu = \nu_1 < \nu_2 = \boldsymbol{\delta}\left(\tfrac{a_2}{b_2}\right),$$

όπου

$$\nu := \max\left\{k \in \mathbb{N}_0 : p^k \mid \rho\right\} = \boldsymbol{\delta}\left(\tfrac{\rho}{b_1}\right) = \boldsymbol{\delta}\left(r\right).$$

Πράγματι· επειδή

$$\rho = p^{\nu_1}a_1' - p^{\nu_2}a_2'\pi \Longrightarrow p^{\nu_1} \mid \rho,$$

συμπεραίνουμε ότι $\nu \geq \nu_1$. Υποθέτοντας ότι $\nu > \nu_1$, καταλήγουμε σε κάτι το άτοπο, καθόσον από τη σχέση διαιρετότητας $p^{\nu} \mid \rho$ έπεται ότι

$$p^{\nu_1}a_1' \equiv p^{\nu_2}a_2'\pi (\mathrm{mod}\, p^{\nu}) \implies a_1' \equiv p^{\nu_2-\nu_1}a_2'\pi (\mathrm{mod}\, p^{\nu-\nu_1})$$
$$\Downarrow$$
$$\exists \lambda \in \mathbb{Z} : a_1' = p(p^{\nu_2-\nu_1-1}a_2'\pi + \lambda p^{\nu-\nu_1-1}),$$

ενώ $p \nmid a_1'$. Άρα όντως $\nu = \nu_1 < \nu_2$ και, βάσει των όσων προαναφέραμε, ο $\mathbb{Z}_{\langle p\rangle}$ καθίσταται ευκλείδεια περιοχή με την p-αδική προσθετική εκτίμηση ως ευκλείδεια στάθμη του.

(iv) Εκτός των (i)-(iii), στην κλάση των ευκλειδείων περιοχών συμπεριλαμβάνονται: ο δακτύλιος $K[\mathsf{X}]$ και ο δακτύλιος των επίτυπων δυναμοσειρών $K[\![\mathsf{X}]\!]$ (όπου K σώμα, βλ. προτάσεις 5.4.8 και 5.4.11), ορισμένες τετραγωνικές αριθμητικές περιοχές (βλ. πρόταση 5.4.16), καθώς και ορισμένοι εκ των δακτυλίων των ακεραίων των τετραγωνικών αριθμητικών σωμάτων. (Βλ. 5.5.7 και 5.5.8).

► **Διαίρεση πολυωνύμων και επίτυπων δυναμοσειρών**. Ο τρόπος εκτελέσεως τής «διαιρέσεως» ενός πολυωνύμου μιας απροσδιορίστου $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ διά ενός πολυωνύμου $\psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$ (όπου K σώμα) είναι γνωστός από το σχολείο και από τις παραδόσεις τής Εισαγωγικής Άλγεβρας. Άμεσες γενικεύσεις τής εν λόγω διαιρέσεως δίδονται στο θεώρημα 5.4.4 και στο πόρισμα 5.4.5.

5.4.4 Θεώρημα. (Γενικευμένος Αλγόριθμος Διαιρέσεως) *Δοθέντων δυο πολυωνύμων*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}], \;\; \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$$

με τους συντελεστές τους ειλημμένους από έναν μεταθετικό δακτύλιο R με μοναδιαίο στοιχείο, όπου $\mathrm{LC}(\psi(\mathsf{X})) = b_m$, *υπάρχει ζεύγος πολυωνύμων $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in R[\mathsf{X}]$, καθώς και ένας $k \in \mathbb{N}_0$, ούτως ώστε να ισχύει*

$$\left(\mathrm{LC}(\psi)\right)^k \cdot \varphi(\mathsf{X}) = \varpi(\mathsf{X}) \cdot \psi\left(\mathsf{X}\right) + \upsilon(\mathsf{X}), \quad \deg\left(\upsilon(\mathsf{X})\right) < \deg\left(\psi\left(\mathsf{X}\right)\right) \tag{5.28}$$

ΑΠΟΔΕΙΞΗ. Εάν $\deg(\varphi(\mathsf{X})) < \deg(\psi(\mathsf{X}))$, τότε θέτοντας $k := 0$, $\varpi(\mathsf{X}) := 0_{R[\mathsf{X}]}$ και $\upsilon(\mathsf{X}) := \varphi(\mathsf{X})$, η (5.28) επαληθεύεται. Από εδώ λοιπόν και στο εξής μπορούμε να υποθέσουμε ότι

$$n = \deg(\varphi(\mathsf{X})) \geq \deg(\psi(\mathsf{X})) = m, \;\; n \geq 0.$$

Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον n. Εάν $n = 0$, τότε $m = 0$ και

$$\varphi(\mathsf{X}) = a_0, \;\; \psi(\mathsf{X}) = b_0,$$

οπότε αρκεί να θέσουμε $\varpi(\mathsf{X}) = a_0$, $\upsilon(\mathsf{X}) = 0_{R[\mathsf{X}]}$ και $k = 1$ για να λάβουμε την (5.28). Εν συνεχεία, υποθέτουμε ότι $n > 0$ και ότι *για κάθε πολυώνυμο* $\chi(\mathsf{X}) \in R[\mathsf{X}]$ *με* $\deg(\chi(\mathsf{X})) < n$ υπάρχει ένα ζεύγος πολυωνύμων $\varpi'(\mathsf{X})$ και $\upsilon'(\mathsf{X}) \in R[\mathsf{X}]$, καθώς και ένας $k' \in \mathbb{N}_0$, ούτως ώστε να ισχύει

$$\left(\mathrm{LC}(\psi(\mathsf{X}))\right)^{k'} \chi(\mathsf{X}) = \varpi'(\mathsf{X})\psi\left(\mathsf{X}\right) + \upsilon'(\mathsf{X}), \quad \deg\left(\upsilon'(\mathsf{X})\right) < \deg\left(\psi\left(\mathsf{X}\right)\right). \tag{5.29}$$

Ορίζουμε ως $\chi(\mathsf{X})$ το[12]

$$\chi(\mathsf{X}) := \left(\mathrm{LC}(\psi(\mathsf{X}))\right)^k \varphi(\mathsf{X}) - a_n \mathsf{X}^{n-m} \psi(\mathsf{X}) \in R[\mathsf{X}].$$

Εάν $\chi(\mathsf{X}) = 0_{R[\mathsf{X}]}$, τότε λαμβάνουμε εκ νέου την (5.28) θέτοντας

$$k := 1, \;\; \varpi(\mathsf{X}) := a_n \mathsf{X}^{n-m}, \;\; \upsilon(\mathsf{X}) := 0_{R[\mathsf{X}]}.$$

Ειδάλλως, εκμεταλλευόμενοι την επαγωγική μας υπόθεση (5.29) θέτουμε

$$\upsilon(\mathsf{X}) := \upsilon'(\mathsf{X}), \;\; \varpi(\mathsf{X}) := \varpi'(\mathsf{X}) + \left(\mathrm{LC}(\psi(\mathsf{X}))\right)^{k'} \left(a_n \mathsf{X}^{n-m}\right), \;\; k := k' + 1,$$

καταλήγοντας στην ισότητα

$$\begin{aligned} \left(\mathrm{LC}(\psi(\mathsf{X}))\right)^k \varphi(\mathsf{X}) &= \left(\mathrm{LC}(\psi(\mathsf{X}))\right)^{k'} \chi(\mathsf{X}) + \left(\mathrm{LC}(\psi(\mathsf{X}))\right)^{k'} \left(a_n \mathsf{X}^{n-m} \psi\left(\mathsf{X}\right)\right) \\ &= \varpi(\mathsf{X})\psi\left(\mathsf{X}\right) + \upsilon(\mathsf{X}), \end{aligned}$$

όπου $\deg\left(\upsilon(\mathsf{X})\right) = \deg\left(\upsilon'(\mathsf{X})\right) < \deg\left(\psi\left(\mathsf{X}\right)\right)$. □

[12] Ο συντελεστής τού προκειμένου $\chi(\mathsf{X})$ είναι ο $b_m a_n - a_n b_m = 0_R$, οπότε $\deg(\chi(\mathsf{X})) < n$.

5.4.5 Πόρισμα. (Αλγόριθμος Διαιρέσεως) *Δοθέντων δυο πολυωνύμων*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}],\ \ \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\},$$

με τους συντελεστές τους ειλημμένους από μια ακεραία περιοχή R, όπου $\mathrm{LC}(\psi(\mathsf{X})) = b_m \in R^\times$*, υπάρχει ένα ζεύγος* ***μονοσημάντως ορισμένων*** *πολυωνύμων* $\varpi(\mathsf{X})$ *και* $\upsilon(\mathsf{X}) \in R[\mathsf{X}]$*, τέτοιων ώστε να ισχύει*

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X}) \cdot \psi(\mathsf{X}) + \upsilon(\mathsf{X}),\ \ \deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X})). \tag{5.30}$$

ΑΠΟΔΕΙΞΗ. Κατά το θεώρημα 5.4.4 υπάρχει ένα ζεύγος πολυωνύμων $\varpi_*(\mathsf{X})$ και $\upsilon_*(\mathsf{X}) \in R[\mathsf{X}]$, καθώς και ένας $k \in \mathbb{N}_0$, ούτως ώστε να ισχύει

$$\left(\mathrm{LC}(\psi(\mathsf{X}))\right)^k \cdot \varphi(\mathsf{X}) = \varpi_*(\mathsf{X}) \cdot \psi(\mathsf{X}) + \upsilon_*(\mathsf{X}),\ \ \deg(\upsilon_*(\mathsf{X})) < \deg(\psi(\mathsf{X})).$$

Επειδή $\mathrm{LC}(\psi) \in R^\times$ (οπότε και $(\mathrm{LC}(\psi))^k \in R^\times$), η (5.30) επαληθεύεται θέτοντας

$$\varpi(\mathsf{X}) := \varpi_*(\mathsf{X}) \left(\mathrm{LC}(\psi(\mathsf{X}))^k\right)^{-1},\ \ \upsilon(\mathsf{X}) := \upsilon_*(\mathsf{X}) \left(\mathrm{LC}(\psi(\mathsf{X}))^k\right)^{-1}.$$

Αρκεί λοιπόν να αποδειχθεί και το *μονοσήμαντο* μιας τέτοιας εκφράσεως. Εάν πέραν των $\varpi(\mathsf{X})$, $\upsilon(\mathsf{X})$ υπάρχουν και άλλα δύο πολυώνυμα $\varpi'(\mathsf{X})$ και $\upsilon'(\mathsf{X})$, τα οποία πλήρουν τις[13]

$$\begin{gathered}\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}) = \varpi'(\mathsf{X})\psi(\mathsf{X}) + \upsilon'(\mathsf{X}),\\ \deg(\upsilon(\mathsf{X})) \le \deg(\upsilon'(\mathsf{X})) < \deg(\psi(\mathsf{X})),\end{gathered}$$

τότε

$$(\varpi(\mathsf{X}) - \varpi'(\mathsf{X}))\,\psi(\mathsf{X}) = \upsilon'(\mathsf{X}) - \upsilon(\mathsf{X}). \tag{5.31}$$

Υποθέτοντας ότι $\upsilon'(\mathsf{X}) \neq \upsilon(\mathsf{X})$, η (5.31) μας πληροφορεί ότι $\varpi(\mathsf{X}) \neq \varpi'(\mathsf{X})$, οπότε με τη βοήθεια τού (i) τού λήμματος 1.3.7 και τού (i) τής προτάσεως 1.3.9 συμπεραίνουμε ότι

$$\deg(\upsilon'(\mathsf{X})) \ge \deg(\upsilon'(\mathsf{X}) - \upsilon(\mathsf{X})) = \deg(\varpi(\mathsf{X}) - \varpi'(\mathsf{X})) + \deg(\psi(\mathsf{X})) \ge \deg(\psi(\mathsf{X})),$$

πράγμα που αντίκειται προς την ανίσωση $\deg(\upsilon'(\mathsf{X})) < \deg(\psi(\mathsf{X}))$. Συνεπώς,

$$\upsilon'(\mathsf{X}) = \upsilon(\mathsf{X}) \underset{(5.31)}{\Longrightarrow} (\varpi(\mathsf{X}) - \varpi'(\mathsf{X}))\,\psi(\mathsf{X}) = 0_{R[\mathsf{X}]} \Rightarrow \varpi(\mathsf{X}) = \varpi'(\mathsf{X}),$$

όπου η τελευταία συνεπαγωγή έπεται από το γεγονός ότι $\psi(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$ και από το ότι ο δακτύλιος $R[\mathsf{X}]$ είναι μια ακεραία περιοχή (βλ. 1.3.9 (ii)). □

[13] Εάν $\deg(\upsilon'(\mathsf{X})) \le \deg(\upsilon(\mathsf{X}))$, τότε επαναλαμβάνουμε τα ίδια αποδεικτικά επιχειρήματα εναλλάσσοντας τους ρόλους των $\upsilon(\mathsf{X})$ και $\upsilon'(\mathsf{X})$.

5.4.6 Ορισμός. Το πολυώνυμο $\varpi(\mathsf{X})$ στον τύπο (5.30) ονομάζεται **πηλίκο** και το $\upsilon(\mathsf{X})$ **υπόλοιπο** τής διαιρέσεως τού $\varphi(\mathsf{X})$ διά τού $\psi(\mathsf{X})$ εντός τού δακτυλίου $R\,[\mathsf{X}]$.

5.4.7 Παράδειγμα. Εάν

$$\varphi(\mathsf{X}) = \mathsf{X}^7 - 2\mathsf{X}^6 + \mathsf{X}^4 - \mathsf{X}^3 + 2\mathsf{X}^2 - 1, \quad \psi(\mathsf{X}) = \mathsf{X}^6 - 2\mathsf{X}^5 + 2\mathsf{X}^2 - 1 \in \mathbb{Z}[\mathsf{X}],$$

τότε

$$\varphi(\mathsf{X}) = \mathsf{X} \cdot \psi(\mathsf{X}) + \left(\mathsf{X}^4 - 3\mathsf{X}^3 + 2\mathsf{X}^2 + \mathsf{X} - 1\right).$$

5.4.8 Πρόταση. *Έστω K ένα σώμα. Τότε ο δακτύλιος των πολυωνύμων μιας απροσδιορίστου $K[\mathsf{X}]$ με συντελεστές ειλημμένους από το K καθίσταται ευκλείδεια περιοχή με την*

$$\boldsymbol{\delta} : K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\} \longrightarrow \mathbb{N}_0, \;\; \varphi(\mathsf{X}) \mapsto \boldsymbol{\delta}\left(\varphi(\mathsf{X})\right) := \deg(\varphi(\mathsf{X})), \tag{5.32}$$

ως ευκλείδεια στάθμη της.

ΑΠΟΔΕΙΞΗ. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, τότε σύμφωνα με το (i) τής προτάσεως 1.3.9 (ή το (i) τού πορίσματος 1.3.10) έχουμε

$$\begin{aligned} \boldsymbol{\delta}\left(\varphi(\mathsf{X})\psi(\mathsf{X})\right) &= \deg\left(\varphi(\mathsf{X})\psi(\mathsf{X})\right) \\ &= \deg\left(\varphi(\mathsf{X})\right) + \deg(\psi(\mathsf{X})) \geq \deg\left(\varphi(\mathsf{X})\right) = \boldsymbol{\delta}\left(\varphi(\mathsf{X})\right), \end{aligned}$$

οπότε η $\boldsymbol{\delta}$ ικανοποιεί τη συνθήκη 5.4.1 (i). Επιπροσθέτως, το πόρισμα 5.4.5 μας πληροφορεί ότι για οιαδήποτε πολυώνυμα $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ και $\psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$ υπάρχουν $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X}) \cdot \psi\left(\mathsf{X}\right) + \upsilon(\mathsf{X}), \quad \deg\left(\upsilon(\mathsf{X})\right) < \deg\left(\psi\left(\mathsf{X}\right)\right).$$

Εάν $\upsilon(\mathsf{X}) \neq 0_{K[\mathsf{X}]}$, τότε $\deg\left(\upsilon(\mathsf{X})\right) = \boldsymbol{\delta}\left(\varphi(\mathsf{X})\right) < \boldsymbol{\delta}\left(\psi(\mathsf{X})\right) = \deg\left(\psi\left(\mathsf{X}\right)\right)$. Κατά συνέπειαν, η $\boldsymbol{\delta}$ ικανοποιεί *και* τη συνθήκη 5.4.1 (ii). □

5.4.9 Σημείωση. (i) Ευλόγως τίθεται το ερώτημα: Γιατί η πρόταση 5.4.8 δεν εξακολουθεί να ισχύει εάν κανείς αντικαταστήσει τον δακτύλιο $K[\mathsf{X}]$ με τον $R\,[\mathsf{X}]$, όπου R οιαδήποτε *ακεραία περιοχή* (αφού, μάλιστα, κατά την αποδεικτική διαδικασία χρησιμοποιήσαμε το (i) τής προτάσεως 1.3.9 και το πόρισμα 5.4.5 που ισχύουν για πολυώνυμα ανήκοντα στον $R\,[\mathsf{X}]$, όπου R τυχούσα *ακεραία περιοχή*); Για την απάντηση αυτού τού ερωτήματος οφείλουμε να ανατρέξουμε σε μια σημαντική λεπτομέρεια που περιλαμβάνεται στη διατύπωση τού πορίσματος 5.4.5. Εάν ο δακτύλιος αναφοράς μας R είναι μια ακεραία περιοχή που *δεν είναι* σώμα, τότε ορίζεται καλώς η (αντίστοιχη) απεικόνιση

$$\boldsymbol{\delta} : R\,[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\} \longrightarrow \mathbb{N}_0, \;\; \varphi(\mathsf{X}) \mapsto \boldsymbol{\delta}\left(\varphi(\mathsf{X})\right) := \deg(\varphi(\mathsf{X})),$$

η οποία ναι μεν ικανοποιεί τη συνθήκη 5.4.1 (i) αλλά δεν ικανοποιεί τη συνθήκη 5.4.1 (ii) για *όλα τα* $\psi(\mathsf{X}) \in R[\mathsf{X}]\setminus\{0_{R[\mathsf{X}]}\}$, παρά μόνον για όσα εξ αυτών έχουν επικεφαλής συντελεστή $\mathrm{LC}(\psi(\mathsf{X})) \in R^\times \subsetneqq R\setminus\{0_R\}$. (Για κάθε σώμα K έχουμε $K^\times = K\setminus\{0_K\}$!) Ως εκ τούτου, εντός τού $R[\mathsf{X}]$ μας επιτρέπεται να διαιρούμε τα πολυώνυμα $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ *μόνον* με εκείνα τα $\psi(\mathsf{X}) \in R[\mathsf{X}]\setminus\{0_{R[\mathsf{X}]}\}$ που διαθέτουν αντιστρέψιμο επικεφαλής συντελεστή!

(ii) Γενικότερα ισχύει το εξής: Έστω R μια ακεραία περιοχή. Τότε ο πολυωνυμικός δακτύλιος $R[\mathsf{X}]$ είναι ευκλείδεια περιοχή *εάν και μόνον εάν* η R είναι σώμα. (Βλ. πρόταση 5.4.24.)

(iii) Η πρόταση 5.4.11 (η οποία μπορεί να εκληφθεί ως το ανάλογο τής προτάσεως 5.4.8 για επίτυπες δυναμοσειρές) μας πληροφορεί ότι ακόμη και ο δακτύλιος των επίτυπων δυναμοσειρών μιας απροσδιορίστου $K[\![\mathsf{X}]\!]$ με συντελεστές ειλημμένους από κάποιο σώμα K καθίσταται *κατά τρόπο φυσικό* ευκλείδεια περιοχή.

5.4.10 Πρόταση. (Αλγόριθμος Διαιρέσεως) *Δοθεισών δυο επίτυπων δυναμοσειρών*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in K[\![\mathsf{X}]\!],\ \ \psi(\mathsf{X}) = \sum_{j=0}^{\infty} b_j \mathsf{X}^j \in K[\![\mathsf{X}]\!]\setminus\{0_{K[\![\mathsf{X}]\!]}\},$$

με τους συντελεστές τους ειλημμένους από ένα σώμα K, υπάρχει ένα ζεύγος επίτυπων δυναμοσειρών $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in K[\![\mathsf{X}]\!]$, τέτοιων ώστε να ισχύει[14]

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X}) \cdot \psi(\mathsf{X}) + \upsilon(\mathsf{X}), \tag{5.33}$$

όπου είτε $\upsilon(\mathsf{X}) = 0_{K[\![\mathsf{X}]\!]}$ είτε $(\upsilon(\mathsf{X}) \neq 0_{K[\![\mathsf{X}]\!]}$ και $\mathrm{ord}(\upsilon(\mathsf{X})) < \mathrm{ord}(\psi(\mathsf{X})))$.

Απόδειξη. Εάν ισχύει $\varphi(\mathsf{X}) = 0_{K[\![\mathsf{X}]\!]}$ ή $\mathrm{ord}(\varphi(\mathsf{X})) < \mathrm{ord}(\psi(\mathsf{X}))$, τότε θέτοντας $\varpi(\mathsf{X}) := 0_{K[\![\mathsf{X}]\!]}$ και $\upsilon(\mathsf{X}) := \varphi(\mathsf{X})$, η (5.33) επαληθεύεται. Από εδώ λοιπόν και στο εξής μπορούμε να υποθέσουμε ότι $\varphi(\mathsf{X}) \neq 0_{K[\![\mathsf{X}]\!]}$ και

$$n = \mathrm{ord}(\varphi(\mathsf{X})) \geq \mathrm{ord}(\psi(\mathsf{X})) = m.$$

Σύμφωνα με το (ii) τού πορίσματος 1.3.10 υπάρχουν (μονοσημάντως ορισμένες) επίτυπες δυναμοσειρές $\chi_1(\mathsf{X}), \chi_2(\mathsf{X}) \in K[\![\mathsf{X}]\!]^\times$, τέτοιες ώστε να ισχύουν οι ισότητες

$$\varphi(\mathsf{X}) = \mathsf{X}^n \chi_1(\mathsf{X}),\ \ \psi(\mathsf{X}) = \mathsf{X}^m \chi_2(\mathsf{X}).$$

Θέτοντας $\varpi(\mathsf{X}) := \chi_1(\mathsf{X})\,(\chi_2(\mathsf{X}))^{-1}\,\mathsf{X}^{n-m}$ και $\upsilon(\mathsf{X}) := 0_{K[\![\mathsf{X}]\!]}$ λαμβάνουμε

$$\begin{aligned} \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}) &= \varpi(\mathsf{X})\psi(\mathsf{X}) \\ &= \left(\chi_1(\mathsf{X})\,(\chi_2(\mathsf{X}))^{-1}\,\mathsf{X}^{n-m}\right)\mathsf{X}^m\chi_2(\mathsf{X}) \\ &= \mathsf{X}^n\chi_1(\mathsf{X}) = \varphi(\mathsf{X}). \end{aligned}$$

[14] Σημειωτέον ότι, εν προκειμένω, όπως θα διαφανεί στην απόδειξη, είτε $\varpi(\mathsf{X}) = 0_{K[\![\mathsf{X}]\!]}$ είτε $\upsilon(\mathsf{X}) = 0_{K[\![\mathsf{X}]\!]}$. Κατά συνέπειαν, για οιεσδήποτε επίτυπες δυναμοσειρές $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\![\mathsf{X}]\!]\setminus\{0_{K[\![\mathsf{X}]\!]}\}$ έχουμε πάντοτε είτε $\varphi(\mathsf{X}) \mid \psi(\mathsf{X})$ είτε $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$!

οπότε η (5.33) επαληθεύεται και σε αυτήν την περίπτωση. □

5.4.11 Πρόταση. *Έστω K ένα σώμα. Τότε ο δακτύλιος των επίτυπων δυναμοσειρών μιας απροσδιορίστου $K[\![\mathsf{X}]\!]$ με συντελεστές ειλημμένους από το K καθίσταται ευκλείδεια περιοχή με την*

$$\boldsymbol{\delta} : K[\![\mathsf{X}]\!]\setminus\{0_{K[\![\mathsf{X}]\!]}\} \longrightarrow \mathbb{N}_0,\ \ \varphi(\mathsf{X}) \mapsto \boldsymbol{\delta}\left(\varphi(\mathsf{X})\right) := \operatorname{ord}(\varphi(\mathsf{X})), \tag{5.34}$$

ως ευκλείδεια στάθμη της.

ΑΠΟΔΕΙΞΗ. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\![\mathsf{X}]\!]\setminus\{0_{K[\![\mathsf{X}]\!]}\}$, τότε σύμφωνα με το (ii) τού πορίσματος 1.3.10 έχουμε

$$\begin{aligned} \boldsymbol{\delta}\left(\varphi(\mathsf{X})\psi(\mathsf{X})\right) &= \operatorname{ord}\left(\varphi(\mathsf{X})\psi(\mathsf{X})\right) \\ &= \operatorname{ord}\left(\varphi(\mathsf{X})\right) + \operatorname{ord}(\psi(\mathsf{X})) \geq \operatorname{ord}\left(\varphi(\mathsf{X})\right) = \boldsymbol{\delta}\left(\varphi(\mathsf{X})\right), \end{aligned}$$

οπότε η $\boldsymbol{\delta}$ ικανοποιεί τη συνθήκη 5.4.1 (i). Επιπροσθέτως, η πρόταση 5.4.11 μας πληροφορεί ότι για οιεσδήποτε $\varphi(\mathsf{X}) \in K[\![\mathsf{X}]\!]$ και $\psi(\mathsf{X}) \in K[\![\mathsf{X}]\!]\setminus\{0_{K[\![\mathsf{X}]\!]}\}$ υπάρχουν $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in K[\![\mathsf{X}]\!]$, τέτοιες ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi\left(\mathsf{X}\right) + \upsilon(\mathsf{X}),$$

όπου είτε $\upsilon(\mathsf{X}) = 0_{K[\![\mathsf{X}]\!]}$ είτε $(\upsilon(\mathsf{X}) \neq 0_{K[\![\mathsf{X}]\!]}$ και $\operatorname{ord}(\upsilon(\mathsf{X})) < \operatorname{ord}(\psi\left(\mathsf{X}\right)))$. Κατά συνέπειαν, η $\boldsymbol{\delta}$ ικανοποιεί *και* τη συνθήκη 5.4.1 (ii). □

► **Κάποιες εκ των περιοχών $\mathbb{Z}[\sqrt{m}]$ είναι ευκλείδειες.** Φυσικό πρόβλημα: Για ποιους ακεραίους αριθμούς m στερουμένους τετραγώνων είναι η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{m}]$ (η ορισθείσα στην άσκηση **1-44**) ευκλείδεια; Το πρόβλημα αυτό είναι δύσκολο, ορισμένες δε πτυχές του παραμένουν ακόμη και σήμερα ιδιαίτερα «σκοτεινές» (βλ. 5.5.9 (ii)). Στην πρόταση 5.4.16 αποδεικνύουμε ότι η $\mathbb{Z}[\sqrt{m}]$ είναι ευκλείδεια περιοχή όταν $m \in \{-2, -1, 2, 3, 6, 7\}$. Γενικεύσεις αυτής παρατίθενται στην ενότητα 5.5 (βλ. θεωρήματα 5.5.7 και 5.5.8).

5.4.12 Ορισμός. Έστω m ένας ακέραιος στερούμενος τετραγώνων. Τότε μια υποπεριοχή R τού τετραγωνικού αριθμητικού σώματος $\mathbb{Q}(\sqrt{m})$ καλείται **N-ευκλείδεια περιοχή** όταν αυτή καθίσταται ευκλείδεια περιοχή με στάθμη της την

$$\boldsymbol{\delta}_{\mathbf{N}} : R\setminus\{0\} \longrightarrow \mathbb{N}_0,\ \ \boldsymbol{\delta}_{\mathbf{N}}\left(z\right) := |\mathbf{N}(z)| = |z\overline{z}|,\ \ \forall z \in R\setminus\{0\}, \tag{5.35}$$

όπου $\mathbf{N}$ η αριθμητική στάθμη τού $\mathbb{Q}(\sqrt{m})$ (βλ. 5.2.38).

5.4.13 Παρατήρηση. Λόγω των ιδιοτήτων 5.2.39 (i) και (ii) τής $\mathbf{N}$ η συνθήκη 5.4.1 (i) ικανοποιείται από την $\boldsymbol{\delta}_{\mathbf{N}}$ για κάθε υποπεριοχή R τού $\mathbb{Q}(\sqrt{m})$. Πράγματι· για οιαδήποτε $z, w \in R\setminus\{0\}$ έχουμε

$$\left.\begin{array}{r} |\mathbf{N}(zw)| = |\mathbf{N}(z)|\,|\mathbf{N}(w)| \\ w \neq 0 \Rightarrow |\mathbf{N}(w)| \geq 1 \end{array}\right\} \Longrightarrow \boldsymbol{\delta}_{\mathbf{N}}\left(zw\right) \geq \boldsymbol{\delta}_{\mathbf{N}}\left(z\right).$$

Ως εκ τούτου, για να είναι μια τέτοια υποπεριοχή $\mathbf{N}$-ευκλείδεια αρκεί να προσδιορισθούν μόνον προϋποθέσεις υπό τις οποίες ικανοποιείται η συνθήκη 5.4.1 (ii). (Για την $R = \mathbb{Z}[\sqrt{m}]$ βλ. λήμμα 5.4.14.)

5.4.14 Λήμμα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν για οιαδήποτε $z \in \mathbb{Z}[\sqrt{m}]$ και $w \in \mathbb{Z}[\sqrt{m}] \setminus \{0\}$, το κλάσμα $\frac{z}{w}$, γραφόμενο υπό τη μορφή*

$$\frac{z}{w} = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m}) = \mathbf{Fr}(\mathbb{Z}[\sqrt{m}]), \;\; x, y \in \mathbb{Q}, \tag{5.36}$$

είναι τέτοιο, ώστε να υπάρχουν $a, b \in \mathbb{Z}$ ικανοποιούντες τη συνθήκη

$$\left|\mathbf{N}((a-x) + (b-y)\sqrt{m})\right| = \left|(a-x)^2 - m(b-y)^2\right| < 1, \tag{5.37}$$

τότε η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{m}]$ είναι $\mathbf{N}$-ευκλείδεια περιοχή.

ΑΠΟΔΕΙΞΗ. Βάσει των προαναφερθέντων στο εδάφιο 5.4.13 αρκεί να αποδειχθεί ότι η $\boldsymbol{\delta}_{\mathbf{N}}$ πληροί τη συνθήκη 5.4.1 (ii). Προς τούτο θεωρούμε τυχόντα στοιχεία $z \in \mathbb{Z}[\sqrt{m}]$ και $w \in \mathbb{Z}[\sqrt{m}] \setminus \{0\}$ και εκφράζουμε το κλάσμα $\frac{z}{w}$ υπό τη μορφή (5.36). Εξ υποθέσεως, υπάρχουν $a, b \in \mathbb{Z}$ ικανοποιούντες τη συνθήκη (5.37). Θέτοντας

$$q := a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}], \;\; r := z - qw \in \mathbb{Z}[\sqrt{m}],$$

παρατηρούμε ότι $z = qw + r$. Στην περίπτωση όπου $r \neq 0$ η (5.37) δίδει

$$\left|\mathbf{N}(\frac{r}{w})\right| = \left|\mathbf{N}(\frac{z}{w} - q)\right| = \left|\mathbf{N}((a-x) + (b-y)\sqrt{m})\right| < 1,$$

οπότε (λόγω των προαναφερθέντων στο εδάφιο 5.2.40)

$$\left|\mathbf{N}(\frac{r}{w})\right| = \left|\frac{\mathbf{N}(r)}{\mathbf{N}(w)}\right| = \frac{|\mathbf{N}(r)|}{|\mathbf{N}(w)|} = \frac{\boldsymbol{\delta}_{\mathbf{N}}(r)}{\boldsymbol{\delta}_{\mathbf{N}}(w)} < 1 \Rightarrow \boldsymbol{\delta}_{\mathbf{N}}(r) < \boldsymbol{\delta}_{\mathbf{N}}(w).$$

Επομένως, η $\boldsymbol{\delta}_{\mathbf{N}}$ πληροί τη συνθήκη 5.4.1 (ii) και η $\mathbb{Z}[\sqrt{m}]$ είναι $\mathbf{N}$-ευκλείδεια περιοχή. □

5.4.15 Λήμμα. *Εάν $\xi \in \mathbb{R}$, $0 \leq \xi < 2$ και $\xi \neq \frac{5}{4}$, τότε για κάθε $x \in \mathbb{R}$ υπάρχει κάποιος $a \in \mathbb{Z}$ για τον οποίο ισχύει*

$$\left|(a-x)^2 - \xi\right| < 1. \tag{5.38}$$

ΑΠΟΔΕΙΞΗ. Θεωρούμε τον $\{x\}_{\text{εγγ}}$ (ήτοι τον ακέραιο το εγγύτερο τού x, βλ. 4.2.10), καθώς και τον $\check{x} := \left|x - \{x\}_{\text{εγγ}}\right|$ με $0 \leq \check{x} \leq \frac{1}{2}$, και θέτουμε

$$a' := \begin{cases} 0, & \text{όταν } 0 \leq \xi < 1, \\ 1, & \text{όταν } 1 \leq \xi < \frac{5}{4}, \\ -1, & \text{όταν } \frac{5}{4} < \xi < 2, \end{cases}$$

και

$$a := \begin{cases} a' - \{x\}_{\varepsilon\gamma\gamma}, & \text{όταν } x \geq \{x\}_{\varepsilon\gamma\gamma}, \\ -a' + \{x\}_{\varepsilon\gamma\gamma}, & \text{όταν } x < \{x\}_{\varepsilon\gamma\gamma}. \end{cases}$$

Προφανώς, $|a - x| = |\check{x} - a'|$, οπότε

$$\left|(a-x)^2 - \xi\right| = \left|(\check{x} - a')^2 - \xi\right|. \tag{5.39}$$

Εάν $0 \leq \xi < 1$, τότε $a' = 0$ και

$$\left.\begin{array}{c} 0 \leq \check{x}^2 \leq \frac{1}{4} \\ -1 < -\xi \leq 0 \end{array}\right\} \Rightarrow -1 < \check{x}^2 - \xi \leq \frac{1}{4} \Rightarrow \left|\check{x}^2 - \xi\right| < 1. \tag{5.40}$$

Εάν $1 \leq \xi < \frac{5}{4}$, τότε $a' = 1$ και

$$\left.\begin{array}{c} \frac{1}{4} \leq (\check{x} - 1)^2 \leq 1 \\ -\frac{5}{4} < -\xi \leq -1 \end{array}\right\} \Rightarrow -1 < (\check{x} - 1)^2 - \xi \leq 0 \Rightarrow \left|(\check{x} - 1)^2 - \xi\right| < 1. \tag{5.41}$$

Εάν $\frac{5}{4} < \xi < 2$, τότε $a' = -1$ και

$$\left.\begin{array}{c} 1 \leq (\check{x} + 1)^2 \leq \frac{9}{4} \\ -2 < -\xi < -\frac{5}{4} \end{array}\right\} \Rightarrow -1 < (\check{x} + 1)^2 - \xi < 1 \Rightarrow \left|(\check{x} + 1)^2 - \xi\right| < 1. \tag{5.42}$$

Από τις (5.39), (5.40), (5.41) και (5.42) έπεται ότι η (5.38) είναι αληθής για τον ως άνω επιλεχθέντα ακέραιο a. □

5.4.16 Πρόταση. *Εάν $m \in \{-2, -1, 2, 3, 6, 7\}$, τότε η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{m}]$ είναι* **N***-ευκλείδεια περιοχή.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε τυχόντα στοιχεία $z \in \mathbb{Z}[\sqrt{m}]$ και $w \in \mathbb{Z}[\sqrt{m}] \setminus \{0\}$, και γράφουμε το κλάσμα $\frac{z}{w}$ υπό τη μορφή

$$\frac{z}{w} = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m}) = \mathbf{Fr}(\mathbb{Z}[\sqrt{m}]), \;\; x, y \in \mathbb{Q}. \tag{5.43}$$

Εν συνεχεία, θέτουμε $b := \{y\}_{\varepsilon\gamma\gamma}$ και διακρίνουμε δύο περιπτώσεις.

Περίπτωση πρώτη. Εάν $m \in \{-2, -1\}$, τότε θέτουμε $a := \{x\}_{\varepsilon\gamma\gamma}$ και παρατηρούμε ότι

$$\left.\begin{array}{l} |a - x| \leq \frac{1}{2} \\ |b - y| \leq \frac{1}{2} \end{array}\right\} \Rightarrow \left|(a-x)^2 - m(b-y)^2\right| \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1.$$

Επομένως, η συνθήκη (5.37) ικανοποιείται και η $\mathbb{Z}[\sqrt{m}]$ είναι **N**-ευκλείδεια περιοχή επί τη βάσει τού λήμματος 5.4.14.

Περίπτωση δεύτερη. Εάν $m \in \{2, 3, 6, 7\}$, τότε έχουμε

$$0 \leq m(b-y)^2 \leq \frac{7}{4} < 2 \;\text{ και }\; \sqrt{\tfrac{5m}{4}} \notin \mathbb{Q} \Rightarrow m(b-y)^2 \neq \frac{5}{4}.$$

Εφαρμόζοντας το λήμμα 5.4.15 για το $\xi := m(b-y)^2$ (και για το x το εμφανιζόμενο στην (5.59)) διασφαλίζουμε την ύπαρξη ενός $a \in \mathbb{Z}$ για τον οποίο ισχύει

$$\left|(a-x)^2 - m(b-y)^2\right| < 1.$$

Επομένως, η συνθήκη (5.37) ικανοποιείται και σε αυτήν την περίπτωση, και η $\mathbb{Z}[\sqrt{m}]$ είναι $\mathbf{N}$-ευκλείδεια περιοχή επί τη βάσει τού λήμματος 5.4.14. □

5.4.17 Παρατήρηση. Σύμφωνα με την πρόταση 5.4.16 ο δακτύλιος των γκαουσιανών ακεραίων $\mathbb{Z}[i]$ είναι $\mathbf{N}$-ευκλείδεια περιοχή. Διαιρώντας τόν $3+2i$ διά τού $1+i$ εντός τού $\mathbb{Z}[i]$ ως προς την (5.35) έχουμε τη δυνατότητα να επιλέξουμε ως πηλίκο q και υπόλοιπο r *διαφορετικούς* μιγαδικούς αριθμούς ανήκοντες στον $\mathbb{Z}[i]$. Επί παραδείγματι,

$$\begin{aligned} 3+2i &= (1+i)(2-i)+i, \\ 3+2i &= (1+i)(3-i)-1, \\ 3+2i &= 2(1+i)+1, \\ 3+2i &= 3(1+i)-i, \end{aligned}$$

όπου *και* στις τέσσερεις περιπτώσεις $\boldsymbol{\delta}_{\mathbf{N}}(r) = 1 < 2 = \boldsymbol{\delta}_{\mathbf{N}}(1+i)$.

► **Γενικές ιδιότητες ευκλειδείων περιοχών**. Στα υπολειπόμενα εδάφια τής παρούσας ενότητας παρατίθενται ορισμένες γενικές ιδιότητες των ευκλειδείων περιοχών. Εξ αφορμής τής παρατηρήσεως 5.4.17 εκκινούμε από την αποσαφήνιση τού πότε τα πηλίκα και τα υπόλοιπα τής διαιρέσεως στοιχείων μιας ευκλείδειας περιοχής R διά μη μηδενικών στοιχείων τής R (ως προς κάποια ευκλείδεια στάθμη $\boldsymbol{\delta}$) είναι *μονοσημάντως ορισμένα*.

5.4.18 Πρόταση. *Έστω R μια ευκλείδεια περιοχή με την $\boldsymbol{\delta} : R\setminus\{0_R\} \longrightarrow \mathbb{N}_0$ ως ευκλείδεια στάθμη της. Τότε η ύπαρξη* μονοσημάντως ορισμένων $(q,r) \in R \times R$, *τα οποία ικανοποιούν την* (5.27) *για οιαδήποτε $a \in R$ και $b \in R\setminus\{0_R\}$, ισοδυναμεί με τη συνθήκη*

$$\boldsymbol{\delta}(c-d) \leq \max\{\boldsymbol{\delta}(c), \boldsymbol{\delta}(d)\},\ \forall\,(c,d) \in (R\setminus\{0_R\}) \times (R\setminus\{0_R\}) : c \neq -d. \quad (5.44)$$

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι υπάρχουν μη μηδενικά, διακεκριμένα στοιχεία c, d τού R, τέτοια ώστε να ισχύει $\boldsymbol{\delta}(c-d) > \max\{\boldsymbol{\delta}(c), \boldsymbol{\delta}(d)\}$. Τότε

$$c = 0_R \cdot (c-d) + c, \quad \boldsymbol{\delta}(c) < \boldsymbol{\delta}(c-d),$$

και $c = 1 \cdot (c-d) + d, \quad \boldsymbol{\delta}(d) < \boldsymbol{\delta}(c-d)$, οπότε το πηλίκο και το υπόλοιπο τής διαιρέσεως τού $a := c$ διά τού $b := c-d$ δεν είναι μονοσημάντως ορισμένο.

Και αντιστρόφως· προϋποθέτοντας την ισχύ τής συνθήκης (5.44) και υποθέτοντας ότι

$$a = q_1 b + r_1, \ \text{ όπου είτε } \ r_1 = 0_R \ \text{ είτε } \ (r_1 \neq 0_R \ \text{ και } \ \boldsymbol{\delta}(r_1) < \boldsymbol{\delta}(b))$$

και

$$a = q_2 b + r_2, \text{ όπου είτε } r_2 = 0_R \text{ είτε } (r_2 \neq 0_R \text{ και } \boldsymbol{\delta}(r_2) < \boldsymbol{\delta}(b))$$

για κάποια $a \in R$ και $b \in R \setminus \{0_R\}$ με $r_1 \neq r_2$ (και, κατ' επέκταση, $q_1 \neq q_2$), συμπεραίνουμε (μέσω τής ιδιότητας (ii) τού ορισμού 5.4.1 για τα $q_1 - q_2$ και b, και τής εφαρμογής τής συνθήκης (5.44) για τα $c := r_1$ και $d := r_2$) ότι

$$\boldsymbol{\delta}(b) \leq \boldsymbol{\delta}((q_1 - q_2) b) = \boldsymbol{\delta}(r_1 - r_2) \leq \max\{\boldsymbol{\delta}(r_1), \boldsymbol{\delta}(r_2)\} < \boldsymbol{\delta}(b),$$

ήτοι κάτι το οποίο είναι άτοπο. Συνεπώς $r_1 = r_2$ και $(q_1 - q_2) b = 0_R \Longrightarrow q_1 = q_2$ (διότι $b \in R \setminus \{0_R\}$, βλ. πρόταση 1.2.5). □

5.4.19 Παρατήρηση. (i) Εντός τού δακτυλίου $\mathbb{Z}[i]$ οι μιγαδικοί αριθμοί $c \in \{\pm 1\}$ και $d \in \{\pm i\}$ δεν πληρούν τη συνθήκη (5.44) ως προς την ευκλείδεια στάθμη (5.35), αφού

$$\boldsymbol{\delta}_{\mathbf{N}}(c - d) = 2 > \max\{\boldsymbol{\delta}_{\mathbf{N}}(c), \boldsymbol{\delta}_{\mathbf{N}}(d)\} = 1.$$

(ii) Παρότι η *συνήθης* ευκλείδεια στάθμη $\boldsymbol{\delta}(= \boldsymbol{\delta}_1) : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}_0$, $\boldsymbol{\delta}(a) := |a|$, τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών (βλ. 5.4.3 (ii)) *δεν* πληροί τη συνθήκη (5.44) για όλα τα ζεύγη μη μηδενικών μη αντιθέτων ακεραίων[15] (c, d), η *μοναδικότητα* τού πηλίκου q και τού υπολοίπου r τής διαιρέσεως ενός $a \in \mathbb{Z}$ διά ενός $b \in \mathbb{Z} \setminus \{0\}$ είναι διασφαλισμένη (στο πλαίσιο τής Στοιχειώδους Θεωρίας Αριθμών) *υπό τις επιπρόσθετες προϋποθέσεις* τού θεωρήματος 5.1.1, διότι σε αυτό αξιώσαμε *από το ίδιο* το εμφανιζόμενο υπόλοιπο r (και όχι μόνον από την απόλυτη τιμή του!) να είναι ≥ 0.

(iii) Έστω K ένα σώμα. Τότε η ευκλείδεια στάθμη (5.32) τού πολυωνυμικού δακτυλίου $K[\mathsf{X}]$ πληροί τη συνθήκη (5.44), οπότε η ιδιότητα τής *μοναδικότητας* των πηλίκων και των υπολοίπων η περιληφθείσα στο πόρισμα 5.4.5 έπεται (εναλλακτικώς) και από την πρόταση 5.4.18.

5.4.20 Πρόταση. *Έστω R μια ευκλείδεια περιοχή με την $\boldsymbol{\delta} : R \setminus \{0_R\} \longrightarrow \mathbb{N}_0$ ως ευκλείδεια στάθμη της. Τότε ισχύουν τα ακόλουθα*:

(i) $\boldsymbol{\delta}(a) \geq \boldsymbol{\delta}(1_R)$, $\forall a \in R \setminus \{0_R\}$.

(ii) *Εάν* $a, b \in R \setminus \{0_R\}$ *και* $a \underset{\text{συν.}}{\sim} b$, *τότε* $\boldsymbol{\delta}(a) = \boldsymbol{\delta}(b)$.

(iii) $\boldsymbol{\delta}(a) = \boldsymbol{\delta}(-a)$, $\forall a \in R \setminus \{0_R\}$.

(iv) $a \in R^\times \Longleftrightarrow a \in R \setminus \{0_R\}$ *και* $\boldsymbol{\delta}(a) = \boldsymbol{\delta}(1_R)$.

[15] Π.χ., για $c = -7$ και $d = 2$ έχουμε $|c - d| = 9 > \max\{|c|, |d|\} = 7$, και για $a := c = -7$ και $b := c - d = -9$ λαμβάνουμε

$$-7 = 0 \cdot (-9) + (-7) = 1 \cdot (-9) + 2 \text{ με } |-7| < |-9|, |2| < |-9|.$$

ΑΠΟΔΕΙΞΗ. (i) Επειδή $a = a \cdot 1_R$, από την ιδιότητα (i) τού ορισμού 5.4.1 λαμβάνουμε $\boldsymbol{\delta}(a) \geq \boldsymbol{\delta}(1_R)$.

(ii) Εάν $a, b \in R \smallsetminus \{0_R\}$ και ισχύει $a \underset{\text{συν.}}{\sim} b$, τότε $a = bx$ για κάποιο $x \in R^\times$. (Βλ. πόρισμα 5.2.5). Προφανώς, $b = ax^{-1}$, οπότε κάνοντας και πάλι χρήση τής ιδιότητας (i) τού ορισμού 5.4.1 λαμβάνουμε

$$\left.\begin{array}{r} \boldsymbol{\delta}(a) = \boldsymbol{\delta}(bx) \geq \boldsymbol{\delta}(b) \\ \boldsymbol{\delta}(b) = \boldsymbol{\delta}\left(ax^{-1}\right) \geq \boldsymbol{\delta}(a) \end{array}\right\} \Longrightarrow \boldsymbol{\delta}(a) = \boldsymbol{\delta}(b).$$

(iii) Επειδή $-a = (-1_R)\, a$ και $a = (-1_R)\,(-a)$, έχουμε $a \underset{\text{συν.}}{\sim} -a$, οπότε αρκεί να εφαρμόσουμε το (ii).

(iv) Εάν $a \in R^\times$, τότε $a \in R \smallsetminus \{0_R\}$ και $\exists! a^{-1} \in R^\times : aa^{-1} = 1_R$, οπότε από το ανωτέρω (i) που έχουμε ήδη αποδείξει και την ιδιότητα (i) τού ορισμού 5.4.1 λαμβάνουμε

$$\left.\begin{array}{r} \boldsymbol{\delta}(a) \geq \boldsymbol{\delta}(1_R) \\ \boldsymbol{\delta}(1_R) = \boldsymbol{\delta}\left(aa^{-1}\right) \geq \boldsymbol{\delta}(a) \end{array}\right\} \Longrightarrow \boldsymbol{\delta}(a) = \boldsymbol{\delta}(1_R).$$

Και αντιστρόφως· εάν $a \in R \smallsetminus \{0_R\}$ και $\boldsymbol{\delta}(a) = \boldsymbol{\delta}(1_R)$, τότε βάσει τής ιδιότητας (ii) τού ορισμού 5.4.1 υπάρχουν $(q, r) \in R \times R$, τέτοια ώστε να ισχύει

$$1_R = qa + r, \;\; \text{όπου είτε } \; r = 0_R \;\; \text{είτε} \;\; (r \neq 0_R \;\text{ και }\; \boldsymbol{\delta}(r) < \boldsymbol{\delta}(a)).$$

Εάν υποθέσουμε ότι $r \neq 0_R$ και $\boldsymbol{\delta}(r) < \boldsymbol{\delta}(a)$, τότε από την υπόθεσή μας και από το ανωτέρω (i) που έχουμε ήδη αποδείξει λαμβάνουμε

$$\boldsymbol{\delta}(1_R) \leq \boldsymbol{\delta}(r) < \boldsymbol{\delta}(a) = \boldsymbol{\delta}(1_R),$$

ήτοι κάτι το οποίο είναι άτοπο. Ως εκ τούτου, $r = 0_R$ και $1_R = qa$, οπότε το a είναι αντιστρέψιμο. □

5.4.21 Θεώρημα. *Κάθε ευκλείδεια περιοχή είναι Π.Κ.Ι.* (*και, κατ' επέκταση, περιοχή με μ.κ.δ.,* βλ. 5.2.34).

ΑΠΟΔΕΙΞΗ. Έστω R μια ευκλείδεια περιοχή με την $\boldsymbol{\delta} : R \smallsetminus \{0_R\} \longrightarrow \mathbb{N}_0$ ως ευκλείδεια στάθμη της. Το τετριμμένο ιδεώδες τής R είναι προφανώς κύριο. Αρκεί λοιπόν να αποδείξουμε ότι και κάθε μη τετριμμένο ιδεώδες τής R είναι κύριο. Υποθέτοντας ότι το I είναι τυχόν μη τετριμμένο ιδεώδες τής R, επιλέγουμε ένα $a \in I \smallsetminus \{0_R\}$, τέτοιο ώστε να ισχύει

$$\boldsymbol{\delta}(a) = \min\{\boldsymbol{\delta}(x) \mid x \in I \smallsetminus \{0_R\}\}.$$

(Το σύνολο $\{\boldsymbol{\delta}(x) \mid x \in I \smallsetminus \{0_R\}\}$, όντας υποσύνολο τού $\mathbb{N}_0$, διαθέτει ελάχιστο στοιχείο.) Θα αποδείξουμε ότι $I = \langle a \rangle$. Προφανώς, $\langle a \rangle \subseteq I$. Εξάλλου, για οιοδήποτε $c \in I$, υπάρχουν $(q, r) \in R \times R$, τέτοια ώστε να ισχύει

$$c = qa + r, \;\; \text{όπου είτε } \; r = 0_R \;\; \text{είτε} \;\; (r \neq 0_R \;\text{ και }\; \boldsymbol{\delta}(r) < \boldsymbol{\delta}(a)).$$

Εάν λοιπόν υποθέσουμε ότι $r \neq 0_R$ και $\boldsymbol{\delta}(r) < \boldsymbol{\delta}(a)$, τότε θα έχουμε

$$r = c - qa \in I \Longrightarrow \boldsymbol{\delta}(r) \in \{\boldsymbol{\delta}(x) \mid x \in I \setminus \{0_R\}\} \Longrightarrow \boldsymbol{\delta}(r) \geq \boldsymbol{\delta}(a),$$

ήτοι κάτι το οποίο είναι άτοπο. Ως εκ τούτου, $r = 0_R$ και $c = qa \in \langle a \rangle \Longrightarrow I \subseteq \langle a \rangle$, οπότε τελικώς $I = \langle a \rangle$. □

5.4.22 Παραδείγματα. Σύμφωνα με το θεώρημα 5.4.21, το (iii) τού εδαφίου 5.4.3 και τις προτάσεις 5.4.8, 5.4.11 και 5.4.16 οι δακτύλιοι

$$\mathbb{Z}_{\langle p \rangle}\ (p \text{ πρώτος}), \quad K[\mathsf{X}],\ K[\![\mathsf{X}]\!]\ (K \text{ σώμα}), \quad \mathbb{Z}[\sqrt{m}],\ m \in \{-2,-1,2,3,6,7\},$$

είναι περιοχές κυρίων ιδεωδών.

5.4.23 Σημείωση. Για ορισμένες *ειδικές ακέραιες περιοχές* ισχύει και το αντίστροφο τού θεωρήματος 5.4.21 (βλ., π.χ., προτάσεις 5.4.24 και 5.4.26). Ωστόσο, αξίζει να επισημανθεί ότι η κλάση των ευκλειδείων περιοχών αποτελεί μια πολύ «ισχνή» υποκλάση τής κλάσεως των περιοχών κυρίων ιδεωδών! Παραδείγματα Π.Κ.Ι. που δεν είναι ευκλείδειες περιοχές δίδονται στην ενότητα 5.5.

5.4.24 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η ακεραία περιοχή $R[\mathsf{X}]$ είναι ευκλείδεια περιοχή.*

(ii) *Η ακεραία περιοχή $R[\mathsf{X}]$ είναι Π.Κ.Ι.*

(iii) *Η ακεραία περιοχή R είναι σώμα.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Τούτο έπεται άμεσα από το θεώρημα 5.4.21.

(ii)⇒(iii) Ο επιμορφισμός δακτυλίων

$$R[\mathsf{X}] \ni \sum_{i=0}^{n} a_i \mathsf{X}^i \longmapsto a_0 \in R$$

έχει ως πυρήνα του το ιδεώδες $\langle \mathsf{X} \rangle$, οπότε το 1ο θεώρημα ισομορφισμών 3.3.3 μας πληροφορεί ότι $R[\mathsf{X}]/\langle \mathsf{X} \rangle \cong R$. Επειδή ο δακτύλιος αναφοράς R είναι εξ υποθέσεως ακεραία περιοχή, το $\langle \mathsf{X} \rangle$ είναι πρώτο ιδεώδες τού δακτυλίου $R[\mathsf{X}]$ (βλ. το (i) τού πορίσματος 3.1.11 και το θεώρημα 2.6.4). Επειδή ο $R[\mathsf{X}]$ είναι εξ υποθέσεως Π.Κ.Ι., το $\langle \mathsf{X} \rangle$ είναι μεγιστικό ιδεώδες του (βλ. την πρόταση 4.2.15 ή το (iv) τού πορίσματος 5.3.5), οπότε η R είναι σώμα (βλ. το (iii) τού πορίσματος 3.1.11 και το πόρισμα 2.6.5).

(iii)⇒(i) Βλ. πρόταση 5.4.8. □

5.4.25 Πόρισμα. *Έστω K ένα σώμα και έστω R μια ακεραία περιοχή που δεν είναι σώμα. Τότε οι ακέραιες περιοχές $\mathbb{Z}[\mathsf{X}]$, $R[\mathsf{X}]$ και*

$$\mathbb{Z}[\mathsf{X}_1, \ldots, \mathsf{X}_n], \quad K[\mathsf{X}_1, \ldots, \mathsf{X}_n], \quad R[\mathsf{X}_1, \ldots, \mathsf{X}_n] \quad (n \geq 2)$$

δεν είναι ούτε ευκλείδειες περιοχές ούτε περιοχές κυρίων ιδεωδών.

5.4.26 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η ακεραία περιοχή $R[\![\mathsf{X}]\!]$ είναι ευκλείδεια περιοχή.*

(ii) *Η ακεραία περιοχή $R[\![\mathsf{X}]\!]$ είναι Π.Κ.Ι.*

(iii) *Η ακεραία περιοχή R είναι σώμα.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Τούτο έπεται άμεσα από το θεώρημα 5.4.21.

(ii)⇒(iii) Ο επιμορφισμός δακτυλίων

$$R[\![\mathsf{X}]\!] \ni \sum_{i=0}^{\infty} a_i \mathsf{X}^i \longmapsto a_0 \in R$$

έχει ως πυρήνα του το ιδεώδες $\langle \mathsf{X} \rangle$, οπότε το 1ο θεώρημα ισομορφισμών 3.3.3 μας πληροφορεί ότι $R[\![\mathsf{X}]\!]/\langle \mathsf{X} \rangle \cong R$. Επειδή ο δακτύλιος αναφοράς R είναι εξ υποθέσεως ακεραία περιοχή, το $\langle \mathsf{X} \rangle$ είναι πρώτο ιδεώδες τού δακτυλίου $R[\![\mathsf{X}]\!]$ (βλ. το (i) τού πορίσματος 3.1.11 και το θεώρημα 2.6.4). Επειδή ο $R[\![\mathsf{X}]\!]$ είναι εξ υποθέσεως Π.Κ.Ι., το $\langle \mathsf{X} \rangle$ είναι μεγιστικό ιδεώδες του (βλ. την πρόταση 4.2.15 ή το 5.3.5 (iv)), οπότε η ακεραία περιοχή R είναι σώμα (βλ. το (iii) τού πορίσματος 3.1.11 και το πόρισμα 2.6.5).

(iii)⇒(i) Βλ. πρόταση 5.4.11. □

5.4.27 Πόρισμα. *Έστω K ένα σώμα και έστω R μια ακεραία περιοχή που δεν είναι σώμα. Τότε οι ακέραιες περιοχές $\mathbb{Z}[\![\mathsf{X}]\!]$, $R[\![\mathsf{X}]\!]$ και*

$$\mathbb{Z}[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!], \quad K[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!], \quad R[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!] \quad (n \geq 2)$$

δεν είναι ούτε ευκλείδειες περιοχές ούτε περιοχές κυρίων ιδεωδών.

► **Ευκλείδειος αλγόριθμος προσδιορισμού ενός μ.κ.δ**. Ο υπολογισμός *ενός* μεγίστου κοινού διαιρέτη τυχόντων μη μηδενικών στοιχείων $r_0 = a, r_1 = b$ μιας ευκλείδειας περιοχής R (ως προς μια δεδομένη ευκλείδεια στάθμη $\boldsymbol{\delta} : R \setminus \{0_R\} \longrightarrow \mathbb{N}_0$) μπορεί να εκτελεσθεί με τη βοήθεια ενός αλγορίθμου, ο οποίος είναι ανάλογος τού *συνήθους* ευκλειδείου αλγορίθμου. Πράγματι· ας υποθέσουμε ότι $\boldsymbol{\delta}(a) \geq \boldsymbol{\delta}(b)$. Βάσει τής ιδιότητας (ii) τού ορισμού 5.4.1 υπάρχουν (όχι κατ' ανάγκην μονοσημάντως ορισμένα) ζεύγη στοιχείων (q_j, r_j), $1 \leq j \leq n+1$, $n \in \mathbb{N}_0$, τής R, ούτως ώστε να ισχύουν οι ισότητες:

$$\begin{cases} r_0 = q_1 r_1 + r_2, & \text{όπου είτε } r_2 = 0_R \text{ είτε } (r_2 \neq 0_R \text{ και } \boldsymbol{\delta}(r_2) < \boldsymbol{\delta}(r_1)), \\ r_1 = q_2 r_2 + r_3, & \text{όπου είτε } r_3 = 0_R \text{ είτε } (r_3 \neq 0_R \text{ και } \boldsymbol{\delta}(r_3) < \boldsymbol{\delta}(r_2)), \\ r_2 = q_3 r_3 + r_4, & \text{όπου είτε } r_4 = 0_R \text{ είτε } (r_4 \neq 0_R \text{ και } \boldsymbol{\delta}(r_4) < \boldsymbol{\delta}(r_3)), \\ \cdots\cdots & \cdots\cdots \\ r_{n-2} = q_{n-1} r_{n-1} + r_n, & \text{όπου είτε } r_n = 0_R \text{ είτε } (r_n \neq 0_R \text{ και } \boldsymbol{\delta}(r_n) < \boldsymbol{\delta}(r_{n-1})), \\ r_{n-1} = q_n r_n + r_{n+1}, & \text{όπου είτε } r_{n+1} = 0_R \text{ είτε } (r_{n+1} \neq 0_R \text{ και } \boldsymbol{\delta}(r_{n+1}) < \boldsymbol{\delta}(r_n)). \end{cases}$$

(*Σύμβαση*: Εάν $\exists r_j$, $j \geq 2$, με $r_j = 0_R$, τότε σταματούμε). Εξ αυτών συνάγεται -ιδιαιτέρως- ότι

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

Εάν υποθέταμε ότι για *κάθε* φυσικό αριθμό n το r_{n+1} είναι $\neq 0_R$, θα καταλήγαμε στο συμπέρασμα ότι μεταξύ τού 0 και τού $\boldsymbol{\delta}(r_0)$ 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 $r_{n_*} \neq 0_R$ και $r_{n_*+1} = 0_R$.

5.4.28 Πρόταση. (Ευκλείδειος αλγόριθμος) *Ο r_{n_*} είναι ένας μέγιστος κοινός διαιρέτης των a και b.*

ΑΠΟΔΕΙΞΗ. Εντός τού $\mathrm{Mat}_{2\times 2}(R)$ ισχύουν οι ισότητες

$$\begin{pmatrix} q_j & 1_R \\ 1_R & 0_R \end{pmatrix}\begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} = \begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix},\ \forall j \in \{1, \ldots, n_*\}.$$

Θέτοντας

$$\mathbf{A} := \prod_{j=1}^{n_*}\begin{pmatrix} q_j & 1_R \\ 1_R & 0_R \end{pmatrix},$$

έχουμε

$$\mathbf{A}\begin{pmatrix} r_{n_*} \\ 0_R \end{pmatrix} = \begin{pmatrix} r_{n_*} \\ 0_R \end{pmatrix}\begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Από αυτήν την ισότητα έπεται ότι $a, b \in \langle r_{n_*}\rangle \Longrightarrow \langle a, b\rangle \subseteq \langle r_{n_*}\rangle$. Επιπροσθέτως, επειδή $\det(\mathbf{A}) = (-1_R)^{n_*} \in R^\times$, ο πίνακας $\mathbf{A}$ είναι αντιστρέψιμος (βλ. 1.2.14), οπότε

$$\begin{pmatrix} r_{n_*} \\ 0_R \end{pmatrix} = \mathbf{A}^{-1}\begin{pmatrix} a \\ b \end{pmatrix} \Longrightarrow r_{n_*} \in Ra + Rb = \langle a, b\rangle \Longrightarrow \langle r_{n_*}\rangle \subseteq \langle a, b\rangle.$$

Άρα $\langle r_{n_*}\rangle = \langle a, b\rangle$, πράγμα που σημαίνει ότι $r_{n_*} \in \mathrm{MK\Delta}_R(a, b)$ βάσει τού θεωρήματος 5.2.14. □

5.4.29 Παραδείγματα. (i) Εφαρμόζοντας τον ευκλείδειο αλγόριθμο 5.4.28 για τα στοιχεία $a = r_0 = 25 - 10i$ και $b = r_1 = 5 + i$ τού δακτυλίου $\mathbb{Z}[i]$ των ακεραίων τού Gauss (ως προς την ευκλείδεια στάθμη (5.35)) λαμβάνουμε

$$\begin{cases} 25 - 10i = (4 - 2i)(5 + i) + (3 - 4i), & \boldsymbol{\delta}_{\mathbf{N}}(3 - 4i) = 25 < 26 = \boldsymbol{\delta}_{\mathbf{N}}(5 + i), \\ 5 + i = (1 + i)(3 - 4i) + (-2 + 2i), & \boldsymbol{\delta}_{\mathbf{N}}(-2 + 2i) = 8 < 25 = \boldsymbol{\delta}_{\mathbf{N}}(3 - 4i), \\ 3 - 4i = (-1)(-2 + 2i) + (1 - 2i), & \boldsymbol{\delta}_{\mathbf{N}}(1 - 2i) = 5 < 8 = \boldsymbol{\delta}_{\mathbf{N}}(-2 + 2i), \\ -2 + 2i = (-1)(1 - 2i) - 1, & \boldsymbol{\delta}_{\mathbf{N}}(-1) = 1 < 5 = \boldsymbol{\delta}_{\mathbf{N}}(1 - 2i), \\ 1 - 2i = (-1 + 2i)(-1) + 0, & \end{cases}$$

απ' όπου συμπεραίνουμε ότι οι μιγαδικοί αριθμοί $25-10i$ και $5+i$ είναι σχετικώς πρώτοι εντός τού $\mathbb{Z}[i]$.

(ii) Εφαρμόζοντας τον ευκλείδειο αλγόριθμο 5.4.28 για τα πολυώνυμα

$$\varphi(\mathsf{X}) = 2\mathsf{X}^4 + 5\mathsf{X}^3 - 5\mathsf{X} - 2 \in \mathbb{Q}[\mathsf{X}], \quad \psi(\mathsf{X}) = 2\mathsf{X}^3 - 3\mathsf{X}^2 - 2\mathsf{X} \in \mathbb{Q}[\mathsf{X}]$$

(ως προς την ευκλείδεια στάθμη (5.32)) λαμβάνουμε

$$\begin{cases} \varphi(\mathsf{X}) = (\mathsf{X}+4)\,\psi(\mathsf{X}) + \left(14\mathsf{X}^2 + 3\mathsf{X} - 2\right), & \deg(4\mathsf{X}^2+3\mathsf{X}-2) = 2 < 3, \\ \psi(\mathsf{X}) = \left(\frac{1}{7}\mathsf{X} - \frac{12}{49}\right)\left(14\mathsf{X}^2 + 3\mathsf{X} - 2\right) & \\ \quad + \left(-\frac{48}{49}\mathsf{X} - \frac{24}{49}\right), & \deg(-\frac{48}{49}\mathsf{X} - \frac{24}{49}) = 1 < 2, \\ 14\mathsf{X}^2 + 3\mathsf{X} - 2 = \left(-\frac{343}{24}\mathsf{X} + \frac{49}{12}\right)\left(-\frac{48}{49}\mathsf{X} - \frac{24}{49}\right), & \end{cases}$$

απ' όπου συμπεραίνουμε ότι

$$-\frac{1}{49}\,(48\mathsf{X}+24) \in \mathrm{MK}\Delta_{\mathbb{Q}[\mathsf{X}]}(\varphi(\mathsf{X}), \psi(\mathsf{X})).$$

Επειδή ο ευρεθείς μέγιστος κοινός διαιρέτης έχει περίπλοκους συντελεστές, είναι προτιμότερο να θεωρήσουμε αντ' αυτού το *μονοσημάντως ορισμένο* μονικό πολυώνυμο[16]

$$\left(-\tfrac{49}{48}\right)\left(-\tfrac{48}{49}\mathsf{X} - \tfrac{24}{49}\right) = \mathsf{X} + \tfrac{1}{2} \in \mathrm{MK}\Delta_{\mathbb{Q}[\mathsf{X}]}(\varphi(\mathsf{X}), \psi(\mathsf{X})).$$

5.5 ΠΕΡΙΟΧΕΣ ΚΥΡΙΩΝ ΙΔΕΩΔΩΝ ΟΙ ΟΠΟΙΕΣ ΔΕΝ ΕΙΝΑΙ ΕΥΚΛΕΙΔΕΙΕΣ ΠΕΡΙΟΧΕΣ

Για να εντοπίσουμε παραδείγματα περιοχών κυρίων ιδεωδών οι οποίες δεν είναι ευκλείδειες περιοχές θα εργασθούμε εντός τής οικογενείας *των δακτυλίων* $\mathfrak{O}_m$ *των ακεραίων των τετραγωνικών αριθμητικών σωμάτων* $\mathbb{Q}(\sqrt{m})$. Για $m < 0$ ο δακτύλιος $\mathfrak{O}_m$ είναι Π.Κ.Ι. αλλά όχι και ευκλείδεια περιοχή εάν και μόνον εάν

$$m \in \{-163, -67, -43, -19\}.$$

(Βλ. πόρισμα 5.5.16.)

5.5.1 Ορισμός. Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Ο **δακτύλιος** $\mathfrak{O}_m$ **των (αλγεβρικών) ακεραίων** τού $\mathbb{Q}(\sqrt{m})$ είναι ο

$$\mathfrak{O}_m := \left\{ t \in \mathbb{Q}(\sqrt{m}) \;\middle|\; t^2 + ct + d = 0, \ \text{για κάποια } c, d \in \mathbb{Z} \right\}.$$

(Είναι εύκολο να ελεγχθεί μέσω τής προτάσεως 5.5.2 ότι ο $\mathfrak{O}_m$ είναι ακεραία περιοχή, υποπεριοχή τού σώματος $\mathbb{C}$ όταν $m < 0$ και υποπεριοχή τού σώματος $\mathbb{R}$ όταν $m > 1$.)

[16] Πολλοί συγγραφείς ορίζουν «**τον**» *μέγιστο κοινό διαιρέτη* δύο πολυωνύμων $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ (K σώμα) ως εκείνο το *μονοσημάντως ορισμένο* στοιχείο τού συνόλου $\mathrm{MK}\Delta_{K[\mathsf{X}]}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ που είναι μονικό πολυώνυμο. (Πρόκειται για το μονικό πολυώνυμο που είναι κοινός διαιρέτης των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$ και διαθέτει τον *μέγιστο δυνατό βαθμό*.)

5.5.2 Πρόταση. *Για οιονδήποτε ακέραιο αριθμό m στερούμενο τετραγώνων έχουμε*[17]

$$\boxed{\mathfrak{O}_m = \begin{cases} \mathbb{Z}[\sqrt{m}], & \text{όταν } m \equiv 2(\mathrm{mod}\,4) \text{ ή } m \equiv 3(\mathrm{mod}\,4), \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}], & \text{όταν } m \equiv 1(\mathrm{mod}\,4), \end{cases}}$$

όπου[18]

$$\mathbb{Z}[\tfrac{1+\sqrt{m}}{2}] = \left\{ a + \tfrac{1+\sqrt{m}}{2} b \;\middle|\; a, b \in \mathbb{Z} \right\} = \left\{ \tfrac{k+l\sqrt{m}}{2} \;\middle|\; k, l \in \mathbb{Z} \text{ και } k \equiv l(\mathrm{mod}\,2) \right\}.$$

ΑΠΟΔΕΙΞΗ. "$\subseteq$": Έστω $t \in \mathbb{Q}(\sqrt{m})$ για το οποίο $t^2 + ct + d = 0$, για κάποια $c, d \in \mathbb{Z}$. Επειδή το t είναι τής μορφής $t = r + s\sqrt{m}$, όπου $r, s \in \mathbb{Q}$, έχουμε

$$\left(r + s\sqrt{m}\right)^2 + c\left(r + s\sqrt{m}\right) + d = 0 \Rightarrow \left(r^2 + s^2 m + cr + d\right) + (2rs + cs)\sqrt{m} = 0,$$

απ' όπου έπεται ότι

$$r^2 + s^2 m + cr + d = 0 \tag{5.45}$$

και

$$(2r + c)\, s = 0. \tag{5.46}$$

(i) Εάν $s = 0$, τότε $r \in \mathbb{Z}$. Πράγματι· γράφοντας το r ως *ανάγωγο* κλάσμα $r = \frac{a}{b}$, $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, με μκδ$(a, b) = 1$, λαμβάνουμε μέσω τής (5.45):

$$\left.\begin{array}{r} cr + r^2 = -d \Longrightarrow cab + a^2 = -db^2 \\ \text{μκδ}\,(a, b) = 1 \end{array}\right\} \Longrightarrow a \mid d,$$

οπότε $cb + a = d'b^2$ για κάποιον $d' \in \mathbb{Z}$. Κατά συνέπειαν,

$$a = d'b^2 - cb \Longrightarrow b \mid a \Longrightarrow t = r \in \mathbb{Z}.$$

(ii) Υποθέτουμε ότι $s \neq 0$. Τότε η (5.46) δίδει

$$2r + c = 0 \Longrightarrow r = \frac{k}{2}, \text{ όπου } k := -c \in \mathbb{Z}, \tag{5.47}$$

[17] Όταν $m \equiv 1(\mathrm{mod}\,4)$, έχουμε $\left(\frac{1+\sqrt{m}}{2}\right)^2 = \left(\frac{1+\sqrt{m}}{2}\right) - \frac{1-m}{4}$, όπου $\frac{1-m}{4} \in \mathbb{Z}$, οπότε κάθε στοιχείο τού υποδακτυλίου $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ τού $\mathbb{Q}(\sqrt{m})$ που προκύπτει ύστερα από προσάρτηση τού $\frac{1+\sqrt{m}}{2}$ στην ακεραία περιοχή $\mathbb{Z}$ εκφράζεται (βάσει τής προτάσεως 1.1.16) ως *ακέραιος γραμμικός συνδυασμός* των 1 και $\frac{1+\sqrt{m}}{2}$. Επιπροσθέτως, η ακεραία περιοχή $\mathbb{Z}[\sqrt{m}]$ περιέχεται *γνησίως* εντός τής $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. (Κάθε στοιχείο $a + b\sqrt{m}$ τής $\mathbb{Z}[\sqrt{m}]$ ισούται με $(a - b) + 2b\left(\frac{1+\sqrt{m}}{2}\right)$.)

[18] Εάν $z = a + \frac{1+\sqrt{m}}{2} b$ με $a, b \in \mathbb{Z}$, τότε $z = \frac{k+l\sqrt{m}}{2}$, όπου $k := 2a + b$ και $l := b$ με $k \equiv l(\mathrm{mod}\,2)$. Και αντιστρόφως· εάν $w = \frac{k+l\sqrt{m}}{2}$ με $k, l \in \mathbb{Z}$ και $k - l = 2s$ για κάποιον $s \in \mathbb{Z}$, τότε $w = a + \frac{1+\sqrt{m}}{2} b$, όπου $a := s$ και $b := l$.

και η (5.45) γράφεται ως

$$s^2m - r^2 + d = 0 \Longrightarrow s^2m - r^2 = -d \in \mathbb{Z}. \tag{5.48}$$

Γράφοντας, εν συνεχεία, το s ως *ανάγωγο* κλάσμα $s = \frac{p}{q}$, $(p,q) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ με μκδ$(p,q) = 1$, λαμβάνουμε μέσω των (5.47) (5.48):

$$4p^2m - k^2q = -4q^2d \Longrightarrow 4p^2m = \left(k^2 - 4d\right) q^2,$$

οπότε

$$\left.\begin{array}{r} q^2 \mid 4p^2m \\ \text{μκδ}\,(p,q) = 1 \Longrightarrow \text{μκδ}\left(p^2, q^2\right) = 1 \end{array}\right\} \Longrightarrow q^2 \mid 4m.$$

Επειδή -εξ υποθέσεως- το m στερείται τετραγώνων, το q ισούται με ± 1 ή ± 2. Ως εκ τούτου, *και* στις δύο περιπτώσεις το s μπορεί να εκφρασθεί υπό τη μορφή

$$s = \tfrac{l}{2}, \text{ για κάποιον } l \in \mathbb{Z} \setminus \{0\}. \tag{5.49}$$

Από τις (5.47), (5.48) και (5.49) έπεται ότι

$$\frac{l^2}{4}m - \frac{k^2}{4} \in \mathbb{Z} \Longleftrightarrow l^2m - k^2 \equiv 0 (\mathrm{mod}\, 4) \Longleftrightarrow l^2m \equiv k^2 (\mathrm{mod}\, 4). \tag{5.50}$$

Σημειωτέον ότι $m \not\equiv 0 (\mathrm{mod}\, 4)$, καθότι το m στερείται τετραγώνων. Οι υπόλοιπες περιπτώσεις θα εξετασθούν χωριστά.

Πρώτη περίπτωση: Εάν $m \equiv 1 (\mathrm{mod}\, 4)$, τότε $l^2m \equiv l^2 (\mathrm{mod}\, 4)$, οπότε η (5.50) καταλήγει στην ισοτιμία

$$l^2 \equiv k^2 (\mathrm{mod}\, 4) \Longleftrightarrow (l-k)\,(l+k) \equiv 0 (\mathrm{mod}\, 4) \Longleftrightarrow k \equiv l (\mathrm{mod}\, 2),$$

απ' όπου συμπεραίνουμε ότι $t \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$.

Δεύτερη περίπτωση: Εάν $m \equiv 2 (\mathrm{mod}\, 4)$, τότε $l^2m \equiv 2l^2 (\mathrm{mod}\, 4)$, οπότε η (5.50) καταλήγει στην ισοτιμία

$$l^2 \equiv 2k^2 (\mathrm{mod}\, 4) \Leftrightarrow l^2 - 2k^2 \equiv 0 (\mathrm{mod}\, 4) \Leftrightarrow (k \equiv 0 (\mathrm{mod}\, 2) \text{ και } l \equiv 0 (\mathrm{mod}\, 2))\,,$$

απ' όπου συμπεραίνουμε ότι $t \in \mathbb{Z}[\sqrt{m}]$.

Τρίτη περίπτωση: Εάν $m \equiv 3 (\mathrm{mod}\, 4)$, τότε $l^2m \equiv 3l^2 (\mathrm{mod}\, 4)$, οπότε η (5.50) καταλήγει στην ισοτιμία

$$l^2 \equiv 3k^2 (\mathrm{mod}\, 4) \Leftrightarrow l^2 - 3k^2 \equiv 0 (\mathrm{mod}\, 4) \Leftrightarrow (k \equiv 0 (\mathrm{mod}\, 2) \text{ και } l \equiv 0 (\mathrm{mod}\, 2))\,,$$

απ' όπου συμπεραίνουμε και πάλι ότι $t \in \mathbb{Z}[\sqrt{m}]$.

"$\supseteq$": Εάν $m \equiv 1 (\mathrm{mod}\, 4)$, και $t = \frac{k+l\sqrt{m}}{2} \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$, όπου $k \equiv l (\mathrm{mod}\, 2)$, τότε προφανώς

$$t^2 - kt + \tfrac{k^2 - l^2m}{4} = 0,$$

όπου $k, \frac{k^2-l^2m}{4} \in \mathbb{Z}$, οπότε $t \in \mathfrak{O}_m$.
Εάν, από την άλλη μεριά, $m \equiv 2$ ή $3 (\mathrm{mod}\, 4)$ και $t = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$, όπου $a, b \in \mathbb{Z}$, τότε

$$t^2 - at + a^2 - b^2 m = 0,$$

όπου $a, a^2 - b^2 m \in \mathbb{Z}$, οπότε και πάλι $t \in \mathfrak{O}_m$. □

5.5.3 Σημείωση. Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων με $m \equiv 1 (\mathrm{mod}\, 4)$. Τότε ισχύουν τα εξής:
(i) Η τιμή τής αριθμητικής στάθμης οιουδήποτε στοιχείου

$$z = a + \tfrac{1+\sqrt{m}}{2} b = \left(a + \tfrac{b}{2}\right) + \tfrac{b}{2}\sqrt{m} \in \mathfrak{O}_m = \mathbb{Z}[\tfrac{1+\sqrt{m}}{2}] \ \ (a, b \in \mathbb{Z})$$

(βλ. 5.2.38) ισούται με

$$\boxed{\mathbf{N}(z) = \left(a + \tfrac{b}{2}\right)^2 - \tfrac{mb^2}{4} = a^2 + ab - \tfrac{(m-1)b^2}{4} \in \mathbb{Z}.}$$

Προφανώς, $\mathbf{N}(z) = 0 \Leftrightarrow z = 0$ και

$$m < 0 \Longrightarrow \mathbf{N}(z) = \left(a + \tfrac{b}{2}\right)^2 + (-\tfrac{m}{4}) b^2 \geq 0. \tag{5.51}$$

(ii) Εάν $z \in \mathfrak{O}_m$, τότε $z \in \mathfrak{O}_m^\times \Longleftrightarrow \mathbf{N}(z) \in \{\pm 1\}$. Πράγματι· εάν $z \in \mathfrak{O}_m^\times$, τότε

$$\left.\begin{array}{r} 1 = \mathbf{N}(1) = \mathbf{N}\left(zz^{-1}\right) = \mathbf{N}(z)\,\mathbf{N}\left(z^{-1}\right) \\ \mathbf{N}(z) \in \mathbb{Z},\ \mathbf{N}\left(z^{-1}\right) \in \mathbb{Z} \end{array}\right\} \Rightarrow \mathbf{N}(z) \in \{\pm 1\}.$$

Και αντιστρόφως· εάν $z = a + \frac{1+\sqrt{m}}{2} b \in \mathfrak{O}_m$ $(a, b \in \mathbb{Z})$ με $\mathbf{N}(z) \in \{\pm 1\}$, τότε

$$z(\mathbf{N}(z)\,\overline{z}) = \left(\left(a + \tfrac{b}{2}\right) + \tfrac{b}{2}\sqrt{m}\right)\left(\mathbf{N}(z)\left(\left(a + \tfrac{b}{2}\right) - \tfrac{b}{2}\sqrt{m}\right)\right) = \mathbf{N}(z)^2 = 1,$$

οπότε το z έχει το $\mathbf{N}(z)\,\overline{z}$ ως αντίστροφό του. Σημειωτέον ότι εάν $\mathbf{N}(z) \in \{\pm p\}$ για κάποιο $z \in \mathfrak{O}_m$, τότε το z είναι ανάγωγο στοιχείο τής $\mathfrak{O}_m$. (Η απόδειξη είναι παρόμοια εκείνης τής προτάσεως 5.3.9.)
(iii) Μέσω τού (ii) είναι δυνατή η περιγραφή τής ομάδας $\mathfrak{O}_m^\times$ των αντιστρεψίμων στοιχείων τής $\mathfrak{O}_m$. Ένα στοιχείο

$$z = a + \tfrac{1+\sqrt{m}}{2} b = \left(a + \tfrac{b}{2}\right) + \tfrac{b}{2}\sqrt{m} \in \mathfrak{O}_m = \mathbb{Z}[\tfrac{1+\sqrt{m}}{2}] \ \ (a, b \in \mathbb{Z})$$

ανήκει στην $\mathfrak{O}_m^\times$ εάν και μόνον εάν το διατεταγμένο ζεύγος $(2a + b, b)$ ανήκει στο σύνολο των $(x, y) \in \mathbb{Z}^2$ που ικανοποιούν είτε τη διοφαντική εξίσωση

$$\boxed{x^2 - my^2 = 4} \tag{5.52}$$

είτε τη διοφαντική εξίσωση[19]

$$\boxed{x^2 - my^2 = -4.} \tag{5.53}$$

Ιδιαιτέρως, όταν $m \leq -3$ η (5.53) δεν διαθέτει καμία ακεραία λύση (αφού ισχύει $x^2 - my^2 \geq 0$ για κάθε $(x, y) \in \mathbb{Z}^2$), ενώ οι μόνες ακέραιες λύσεις τής (5.52) είναι οι $(\pm 2, 0)$ για $m \leq -7$ (αφού $y \neq 0 \Rightarrow x^2 - my^2 > 6$) και οι

$$(-2, 0), (2, 0), (1, 1), (-1, 1), (1, -1), (-1, -1)$$

για $m = -3$. Επομένως,

$$\boxed{m \equiv 1 (\mathrm{mod}\, 4) \Rightarrow \mathfrak{O}_m^\times = \begin{cases} \{\pm 1\}, & \text{όταν } m \leq -7, \\ \left\{ \zeta_6^k \,|k \in \{0, 1, 2, 3, 4, 5\} \right\}, & \text{όταν } m = -3, \end{cases}}$$

όπου $\zeta_6 := \exp(\frac{2\pi i}{6}) = \frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

5.5.4 Λήμμα. *Έστω R μια ευκλείδεια περιοχή. Τότε $\exists u \in R \smallsetminus (R^\times \cup \{0_R\})$ με την εξής ιδιότητα: Για κάθε $z \in R$ υπάρχει ένα στοιχείο $r \in R^\times \cup \{0_R\}$ με $u \mid z - r$.*

ΑΠΟΔΕΙΞΗ. Έστω R μια ευκλείδεια περιοχή με την $\boldsymbol{\delta} : R \smallsetminus \{0_R\} \longrightarrow \mathbb{N}_0$ ως ευκλείδεια στάθμη της. Επιλέγουμε κάποιο στοιχείο $u \in R \smallsetminus (R^\times \cup \{0_R\})$, τέτοιο ώστε να ισχύει

$$\boldsymbol{\delta}(u) = \min \left\{ \boldsymbol{\delta}(s) \mid s \in R \smallsetminus (R^\times \cup \{0_R\}) \right\}.$$

Για κάθε $z \in R$ υπάρχουν $(q, r) \in R \times R$ με $z = uq + r$, όπου *είτε* $r = 0_R$ *είτε* $r \neq 0_R$ και $\boldsymbol{\delta}(r) < \boldsymbol{\delta}(u)$. Λόγω τού τρόπου επιλογής τού u έχουμε κατ' ανάγκην $r \in R^\times \cup \{0_R\}$. Επιπροσθέτως, είναι πρόδηλο ότι $u \mid z - r$. □

5.5.5 Λήμμα. *Έστω m ένας ακέραιος στερούμενος τετραγώνων. Εάν $m \leq -13$, τότε η ακεραία περιοχή $\mathfrak{O}_m$ δεν είναι ευκλείδεια περιοχή.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι υπάρχει κάποιος ακέραιος $m \leq -13$ στερούμενος τετραγώνων, τέτοιος ώστε η $\mathfrak{O}_m$ να είναι ευκλείδεια περιοχή. Σημειωτέον ότι ισχύει $\mathfrak{O}_m^\times = \{\pm 1\}$ (βλ. 5.2.41 (i) όταν $m \not\equiv 1 (\mathrm{mod}\, 4)$ και 5.5.3 (iii) όταν $m \equiv 1 (\mathrm{mod}\, 4)$). Σύμφωνα με το λήμμα 5.5.4 υπάρχει κάποιο στοιχείο $u \in \mathfrak{O}_m \smallsetminus \{0, \pm 1\}$ με την εξής ιδιότητα: Για κάθε $z \in \mathfrak{O}_m$ $\exists r \in \{0, \pm 1\}$ με $u \mid z - r$. Αυτό σημαίνει ότι *για κάθε* $z \in \mathfrak{O}_m$ έχουμε

$$u \mid z \text{ ή } u \mid z - 1 \text{ ή } u \mid z + 1. \tag{5.54}$$

[19] Για τον προσδιορισμό των λύσεων των (5.52) και (5.53) μέσω ειδικών αλγορίθμων όταν $m > 1$, βλ.
K.R. Matthews, *The diophantine equation* $x^2 - Dy^2 = N$, $D > 1$, *in integers*, Exp. Math., **18** (2000), 323-331,
R.A. Mollin: *Simple continued fraction solutions of diophantine equations*, Exp. Mathematicae **19** (2001), 55-73, και
J.P. Robertson: *Solving the generalized Pell equation* $x^2 - Dy^2 = N$, manuscript, 2004.

Εφαρμόζοντας τις συνθήκες διαιρετότητας (5.54) για την *ειδική* τιμή $z = 2$ λαμβάνουμε[20] $u \mid 2$ ή $u \mid 3$, οπότε

$$\exists v \in \mathfrak{O}_m : uv \in \{2, 3\}. \tag{5.55}$$

Επειδή $\mathbf{N}(2) = 4$ και $\mathbf{N}(3) = 9,$ από το (5.55) έπεται ότι

$$\mathbf{N}(uv) \in \{4, 9\}. \tag{5.56}$$

Έστω ότι

$$u = \begin{cases} a + b\sqrt{m}, & \text{όταν } m \not\equiv 1 (\mathrm{mod}\, 4), \\ a + \frac{1+\sqrt{m}}{2} b, & \text{όταν } m \equiv 1 (\mathrm{mod}\, 4), \end{cases}$$

και

$$v = \begin{cases} a' + b'\sqrt{m}, & \text{όταν } m \not\equiv 1 (\mathrm{mod}\, 4), \\ a' + \frac{1+\sqrt{m}}{2} b', & \text{όταν } m \equiv 1 (\mathrm{mod}\, 4), \end{cases}$$

για κατάλληλους $a, b, a', b' \in \mathbb{Z}$. Εάν ίσχυε $u \in \mathfrak{O}_m \setminus \mathbb{Z}$ (ήτοι $b \neq 0$) τότε θα είχαμε (λόγω τού (5.55)) $v \in \mathfrak{O}_m \setminus \mathbb{Z}$ (ήτοι $b' \neq 0$) με

$$\mathbf{N}(u) = \begin{cases} a^2 - mb, & \text{όταν } m \not\equiv 1 (\mathrm{mod}\, 4), \\ \left(a + \frac{b}{2}\right)^2 - \frac{mb^2}{4}, & \text{όταν } m \equiv 1 (\mathrm{mod}\, 4), \end{cases}$$

οπότε

$$\mathbf{N}(u) \geq 13 \text{ όταν } m \not\equiv 1 (\mathrm{mod}\, 4) \text{ και } \mathbf{N}(u) \geq \frac{13}{4} > 3 \text{ όταν } m \equiv 1 (\mathrm{mod}\, 4)$$

και (κατ' αναλογίαν)

$$\mathbf{N}(v) \geq 13 \text{ όταν } m \not\equiv 1 (\mathrm{mod}\, 4) \text{ και } \mathbf{N}(v) > 3 \text{ όταν } m \equiv 1 (\mathrm{mod}\, 4).$$

Άρα σε κάθε περίπτωση θα ίσχυε

$$\left.\begin{matrix} \mathbf{N}(u) > 3 \\ \mathbf{N}(v) > 3 \end{matrix}\right\} \Longrightarrow \mathbf{N}(uv) = \mathbf{N}(u)\mathbf{N}(v) > 9,$$

κάτι που θα αντέκειτο προς το (5.56). Κατά συνέπειαν, $u \in \mathbb{Z}$ (ήτοι $b = 0$) και (λόγω τού (5.55)) $v \in \mathbb{Z}$ (ήτοι $b' = 0$). Επειδή (εξ υποθέσεως) $u \notin \{0, \pm 1\}$ έχουμε

$$\left.\begin{matrix} u \in \mathbb{Z} \setminus \{0, \pm 1\}, v \in \mathbb{Z} \\ uv = aa' \in \{2, 3\} \end{matrix}\right\} \Rightarrow u \in \{\pm 2, \pm 3\},\ v \in \{\pm 1\}. \tag{5.57}$$

[20] Το ενδεχόμενο $u \mid 1$ αποκλείεται, διότι εξ υποθέσεως $u \notin \mathfrak{O}_m^{\times}$.

Εν συνεχεία, εφαρμόζοντας τις συνθήκες διαιρετότητας (5.54) για την *ειδική* τιμή

$$z=\begin{cases} 1+\sqrt{m}, & \text{όταν } m\not\equiv 1(\mathrm{mod}\,4),\\ \frac{1+\sqrt{m}}{2}, & \text{όταν } m\equiv 1(\mathrm{mod}\,4),\end{cases}$$

λαμβάνουμε (μέσω τού (5.57))

$$\pm 2\mid z \text{ ή } \pm 2\mid z-1 \text{ ή } \pm 2\mid z+1 \text{ ή } \pm 3\mid z \text{ ή } \pm 3\mid z-1 \text{ ή } \pm 3\mid z+1. \tag{5.58}$$

Εάν υποθέσουμε ότι $\pm 2\mid z$, τότε θα πρέπει να υπάρχουν $\mu,\nu\in\mathbb{Z}$ με

$$z=\begin{cases} \pm 2(\mu+\nu\sqrt{m}), & \text{όταν } m\not\equiv 1(\mathrm{mod}\,4),\\ \pm 2(\mu+\frac{1+\sqrt{m}}{2}\nu), & \text{όταν } m\equiv 1(\mathrm{mod}\,4),\end{cases}$$

πράγμα αδύνατον, καθόσον $\nexists\nu\in\mathbb{Z}:\pm 2\nu=1$. Παρομοίως αποδεικνύεται ότι δεν ικανοποιείται καμία εκ των υπολοίπων συνθηκών (5.58). Επομένως καταλήγουμε σε άτοπο! Ως εκ τούτου, η $\mathfrak{O}_m$ δεν είναι ευκλείδεια περιοχή. □

5.5.6 Λήμμα. *Έστω m ένας ακέραιος στερούμενος τετραγώνων με $m\equiv 1(\mathrm{mod}\,4)$. Εάν για οιαδήποτε $z\in\mathfrak{O}_m$ και $w\in\mathfrak{O}_m\setminus\{0\}$, το κλάσμα $\frac{z}{w}=zw^{-1}$, γραφόμενο υπό τη μορφή*

$$\frac{z}{w}=x+\left(\tfrac{1+\sqrt{m}}{2}\right)y=\left(x+\tfrac{y}{2}\right)+\tfrac{y}{2}\sqrt{m}\in\mathbb{Q}(\sqrt{m}),\ \ x,y\in\mathbb{Q}, \tag{5.59}$$

είναι τέτοιο, ώστε να υπάρχουν $a,b\in\mathbb{Z}$ ικανοποιούντες τη συνθήκη

$$\begin{aligned}\left|\mathbf{N}((a-x)+(b-y)\tfrac{1+\sqrt{m}}{2})\right| &= \left|(a-x)^2+(a-x)(b-y)-\tfrac{(m-1)(b-y)^2}{4}\right|\\ &= \left|\left((a-x)+\tfrac{1}{2}(b-y)\right)^2-\tfrac{m(b-y)^2}{4}\right|<1,\end{aligned} \tag{5.60}$$

τότε η $\mathfrak{O}_m$ είναι $\mathbf{N}$-ευκλείδεια περιοχή.

ΑΠΟΔΕΙΞΗ. Βάσει των προαναφερθέντων στο εδάφιο 5.4.13 αρκεί να αποδειχθεί ότι η απεικόνιση $\boldsymbol{\delta}_{\mathbf{N}}$ πληροί τη συνθήκη 5.4.1 (ii). Προς τούτο θεωρούμε τυχόντα στοιχεία $z\in\mathfrak{O}_m$ και $w\in\mathfrak{O}_m\setminus\{0\}$ και εκφράζουμε το κλάσμα $\frac{z}{w}=zw^{-1}$ υπό τη μορφή (5.59). Εξ υποθέσεως, υπάρχουν $a,b\in\mathbb{Z}$ ικανοποιούντες τη συνθήκη (5.37). Θέτοντας

$$q:=a+b\tfrac{1+\sqrt{m}}{2}\in\mathfrak{O}_m,\ \ r:=z-qw\in\mathfrak{O}_m,$$

παρατηρούμε ότι $z=qw+r$. Στην περίπτωση όπου $r\neq 0$ η (5.37) δίδει

$$\left|\mathbf{N}(\frac{r}{w})\right|=\left|\mathbf{N}(\frac{z}{w}-q)\right|=\left|\mathbf{N}((a-x)+(b-y)\tfrac{1+\sqrt{m}}{2})\right|<1,$$

οπότε (λόγω των προαναφερθέντων στο εδάφιο 5.2.40)

$$\left|\mathbf{N}(\frac{r}{w})\right|=\left|\frac{\mathbf{N}(r)}{\mathbf{N}(w)}\right|=\frac{|\mathbf{N}(r)|}{|\mathbf{N}(w)|}=\frac{\boldsymbol{\delta}_{\mathbf{N}}(r)}{\boldsymbol{\delta}_{\mathbf{N}}(w)}<1\Rightarrow\boldsymbol{\delta}_{\mathbf{N}}(r)<\boldsymbol{\delta}_{\mathbf{N}}(w).$$

Επομένως, η απεικόνιση $\boldsymbol{\delta}_{\mathbf{N}}$ πληροί τη συνθήκη 5.4.1 (ii) και η $\mathfrak{O}_m$ είναι $\mathbf{N}$-ευκλείδεια περιοχή. □

5.5.7 Θεώρημα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν $m<0$, τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η ακεραία περιοχή $\mathfrak{O}_m$ είναι* **N***-ευκλείδεια περιοχή.*

(ii) *Η ακεραία περιοχή $\mathfrak{O}_m$ είναι ευκλείδεια περιοχή.*

(iii) $m\in\{-11,-7,-3,-2,-1\}$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Προφανές.

(ii)⇒(iii) Κατά το λήμμα 5.5.5, $m>-13$, δηλαδή

$$m\in\{-11,-10,-7,-6,-5,-3,-2,-1\}.$$

Όταν $m\in\{-10,-6,-5\}$, τότε προφανώς $m\le -3$, $m\not\equiv 1(\mathrm{mod}\,4)$ και η ακεραία περιοχή $\mathfrak{O}_m=\mathbb{Z}[\sqrt{m}]$ δεν είναι Π.Κ.Ι. (βλ. πρόταση 5.5.2 και το (iii) τής προτάσεως 5.3.8). Ως εκ τούτου, όταν $m\in\{-10,-6,-5\}$ η $\mathfrak{O}_m=\mathbb{Z}[\sqrt{m}]$ δεν είναι ευκλείδεια περιοχή (βλ. θεώρημα 5.4.21). Άρα $m\in\{-11,-7,-3,-2,-1\}$.

(iii)⇒(i) Επειδή

$$-2\equiv 2(\mathrm{mod}\,4),\ -1\equiv 3(\mathrm{mod}\,4),$$

έχουμε $\mathfrak{O}_m=\mathbb{Z}[\sqrt{m}]$ όταν $m\in\{-2,-1\}$. Επομένως, για $m\in\{-2,-1\}$ η ακεραία περιοχή $\mathfrak{O}_m$ είναι **N**-ευκλείδεια περιοχή επί τη βάσει τής προτάσεως 5.4.16. Έστω τώρα ότι $m\in\{-11,-7,-3\}$. Προφανώς, $m\equiv 1(\mathrm{mod}\,4)$ και $\mathfrak{O}_m=\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. Θεωρούμε τυχόντα στοιχεία $z\in\mathfrak{O}_m$ και $w\in\mathfrak{O}_m\setminus\{0\}$ και εκφράζουμε το κλάσμα $\frac{z}{w}=zw^{-1}$ υπό τη μορφή

$$\frac{z}{w}=x+\left(\tfrac{1+\sqrt{m}}{2}\right)y=\left(x+\tfrac{y}{2}\right)+\tfrac{y}{2}\sqrt{m}\in\mathbb{Q}(\sqrt{m}),\ \ x,y\in\mathbb{Q}.$$

Θέτοντας $b:=\{y\}_{\varepsilon\gamma\gamma}$ και $a:=\{x-\frac{1}{2}(b-y)\}_{\varepsilon\gamma\gamma}$ παρατηρούμε ότι

$$\left|\mathbf{N}((a-x)+(b-y)\tfrac{1+\sqrt{m}}{2})\right|=\left|\left((a-x)+\frac{1}{2}(b-y)\right)^2-\tfrac{m(b-y)^2}{4}\right|\le\tfrac{1}{4}+\tfrac{11}{16}<1.$$

Επομένως, η συνθήκη (5.60) ικανοποιείται και η $\mathfrak{O}_m$ είναι **N**-ευκλείδεια περιοχή επί τη βάσει τού λήμματος 5.5.6. □

Μέσω τού θεωρήματος 5.5.7 επιτυγχάνεται πλήρης προσδιορισμός όσων εκ των $\mathfrak{O}_m$ είναι ευκλείδειες περιοχές όταν $m<0$. Αντιθέτως, όταν $m>1$, είναι γνωστό μόνον το ακόλουθο:

5.5.8 Θεώρημα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν $m>1$, τότε η $\mathfrak{O}_m$ είναι* **N***-ευκλείδεια περιοχή εάν και μόνον εάν*

$$m\in\{2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73\}.$$

5.5.9 Σημείωση. (i) Ο προσδιορισμός των **N**-ευκλειδείων περιοχών $\mathfrak{O}_m$ των ακεραίων τού $\mathbb{Q}(\sqrt{m})$ για $m > 1$ διήνυσε μια μακρά ιστορική διαδρομή και απασχόλησε πληθώρα μαθηματικών. Ο Dickson[21] απέδειξε ότι η $\mathfrak{O}_m$ είναι **N**-ευκλείδεια για $m = 2,\ 3,\ 5,\ 13$ (έχοντας λανθασμένως εικάσει τη μη ύπαρξη άλλων). Ο Perron[22] προσέθεσε στον κατάλογο τους $6,\ 7,\ 11,\ 17,\ 21$ και 29. Εν συνεχεία, οι Oppenheimer, Remak και Rédei προσέθεσαν τους υπολοίπους. (Ο Rédei είκασε ότι στον κατάλογο θα ανήκει και το 97, κάτι που κατερρίφθη αργότερα μέσω εργασιών των Barnes και Swinnerton-Dyer.) Βεβαίως, το ότι ο προσδιοριστέος κατάλογος είναι *πεπερασμένος* προέκυπτε ήδη από εργασίες τού Heilbronn δημοσιευθείσες στις αρχές τής δεκαετίας τού 1930. Ωστόσο, η συνθήκη τού «μόνο εάν» τού θεωρήματος 5.5.8 απεδείχθη πλήρως από τους Chatland και Davenport[23], και -ανεξαρτήτως- από τον Inkeri[24] στα μέσα τού 20ου αιώνα.

(ii) Στην περίπτωση όπου $m > 1$ (και σε αντίθεση με ό,τι συμβαίνει όταν $m < 0$) υπάρχουν ευκλείδειες περιοχές $\mathfrak{O}_m$ που *δεν είναι* **N**-ευκλείδειες. Επί παραδείγματι, το 1994 ο Clark[25] απέδειξε ότι η $\mathfrak{O}_{69}$ (με $69 \equiv 1(\mathrm{mod}\,4)$) είναι ευκλείδεια περιοχή με την

$$\boldsymbol{\delta} : \mathfrak{O}_{69}\setminus\{0\} \longrightarrow \mathbb{N}_0,\ \boldsymbol{\delta}\,(z) := \begin{cases} \left|a^2 + ab - 17b^2\right|, & \text{όταν } (a,b) \neq (10,3), \\ 26, & \text{όταν } (a,b) = (10,3), \end{cases}$$

ως ευκλείδεια στάθμη της για κάθε $z = a + \frac{1+\sqrt{69}}{2}b \in \mathfrak{O}_{69}$ $(a, b \in \mathbb{Z})$.

5.5.10 Λήμμα. *Έστω R μια ακεραία περιοχή. Υποθέτουμε ότι υφίσταται απεικόνιση $\boldsymbol{\eta} : R \longrightarrow \mathbb{N}_0$ η οποία ικανοποιεί την εξής συνθήκη: Για κάθε $y \in R\setminus\{0_R\}$ και για κάθε $x \in R$ με $y \nmid x$ υπάρχουν κάποια στοιχεία $u, t \in R$, ούτως ώστε να ισχύουν οι ανισότητες*

$$\boldsymbol{\eta}(0_R) < \boldsymbol{\eta}(xu - yt) < \boldsymbol{\eta}(y). \tag{5.61}$$

Τότε η R είναι Π.Κ.Ι.

ΑΠΟΔΕΙΞΗ. Το τετριμμένο ιδεώδες τής R είναι προφανώς κύριο. Αρκεί λοιπόν να αποδείξουμε ότι και κάθε μη τετριμμένο ιδεώδες τής R είναι κύριο. Υποθέτοντας ότι το I είναι τυχόν μη τετριμμένο ιδεώδες τής R, επιλέγουμε ένα $y \in I\setminus\{0_R\}$, τέτοιο ώστε να ισχύει

$$\boldsymbol{\eta}\,(y) = \min\{\,\boldsymbol{\eta}\,(z) \mid z \in I\setminus\{0_R\}\}\,.$$

[21] Dickson L.E.: *Algebren und ihre Zahlentheorie*, Orell Füssli Verlag, Zürich und Leipzig, 1927.

[22] Perron O.: *Quadratische Zahlkörper mit Euklidischem Algorithmus*,Math. Annalen 107, (1932), 489-495.

[23] Chatland H. and Davenport H.: *Euclid's algorithm in real quadratic fields*, Canad. J. Math. **2**, (1950), 289-296.

[24] Inkeri K.: *Über den Euklidischen Algorithmus in quadratischen Zahlkörpern*, Ann. Acad. Scient. Fennicae, Vol. **41** (1947).

[25] Βλ. Clark D.A.: *A quadratic field which is euclidean but not norm-euclidean*, Manuscripta Math. **83**, (1994), 327-330.

(Το σύνολο $\{\boldsymbol{\eta}(z) \mid z \in I \setminus \{0_R\}\}$, όντας υποσύνολο τού $\mathbb{N}_0$, διαθέτει ελάχιστο στοιχείο.) Θα αποδείξουμε ότι $I = \langle y \rangle$ κάνοντας χρήση τής «εις άτοπον απαγωγής». Προφανώς, $\langle y \rangle \subseteq I$. Ας υποθέσουμε ότι $\langle y \rangle \subsetneqq I$. Θεωρούμε τυχόν $x \in I \setminus \langle y \rangle$. Επειδή $y \nmid x$, υπάρχουν (εξ υποθέσεως) κάποια στοιχεία $u, t \in R$, ούτως ώστε να ισχύουν οι ανισότητες (5.61). Επομένως,

$$\left.\begin{array}{r} u \in R, x \in I \Rightarrow xu \in I \\ t \in R, y \in I \Rightarrow yt \in I \end{array}\right\} \Rightarrow xu - yt \in I.$$

Επειδή $\boldsymbol{\eta}(0_R) < \boldsymbol{\eta}(xu - yt)$, έχουμε κατ' ανάγκην $xu - yt \neq 0_R$, οπότε (λόγω τού τρόπου επιλογής τού y)

$$xu - yt \in I \setminus \{0_R\} \Rightarrow \boldsymbol{\eta}(xu - yt) \geq \boldsymbol{\eta}(y).$$

Τούτο μας οδηγεί σε άτοπο (διότι αντίκειται στη δεύτερη εκ των ανισοτήτων (5.61)). Τελικώς λοιπόν $I = \langle y \rangle$ και η R είναι Π.Κ.Ι. □

5.5.11 Λήμμα. *Έστω m ένας αρνητικός ακέραιος αριθμός στερούμενος τετραγώνων. Εάν για κάθε $y \in \mathfrak{O}_m \setminus \{0_R\}$ και για κάθε $x \in \mathfrak{O}_m$ με $y \nmid x$ υπάρχουν κάποια στοιχεία $u, t \in \mathfrak{O}_m$, ούτως ώστε να ισχύουν οι ανισότητες*

$$0 < \mathbf{N}\left(\frac{x}{y}u - t\right) < 1, \tag{5.62}$$

τότε η $\mathfrak{O}_m$ είναι Π.Κ.Ι.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα ύστερα από εφαρμογή τού λήμματος 5.5.10 για την ακεραία περιοχή $R = \mathfrak{O}_m$ και για την απεικόνιση

$$\boldsymbol{\eta} : \mathfrak{O}_m \longrightarrow \mathbb{N}_0, \;\; z \longmapsto \boldsymbol{\eta}(z) := \mathbf{N}(z),$$

λαμβανομένων υπ' όψιν των ιδιοτήτων τής αριθμητικής στάθμης $\mathbf{N}$ που έχουν προαναφερθεί στα εδάφια 5.2.39 (i), (v) και 5.2.40. Εν προκειμένω, οι ανισότητες (5.61) είναι ισοδύναμες με τις (5.62). □

5.5.12 Πρόταση. (Gauss) *Εάν $m \in \{-163, -67, -43, -19, -11, -7, -3, -2, -1\}$, τότε η ακεραία περιοχή $\mathfrak{O}_m$ είναι Π.Κ.Ι.*

ΑΠΟΔΕΙΞΗ. Εάν

$$m \in \{-11, -7, -3, -2, -1\},$$

τότε σύμφωνα με το θεώρημα 5.5.7 η $\mathfrak{O}_m$ είναι ευκλείδεια περιοχή και, ως εκ τούτου, Π.Κ.Ι. (βλ. θεώρημα 5.4.21). Γι' αυτόν τον λόγο θα υποθέσουμε εφεξής ότι

$$m \in \{-163, -67, -43, -19\}.$$

Προφανώς, $m \equiv 1(\mathrm{mod}\, 4)$ και $\mathfrak{O}_m = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. Θεωρώντας $y \in \mathfrak{O}_m \setminus \{0_R\}$ και $x \in \mathfrak{O}_m$ με $y \nmid x$ γράφουμε το κλάσμα $\frac{x}{y}$ υπό τη μορφή

$$\frac{x}{y} = \frac{\lambda + \mu\sqrt{m}}{\nu}, \text{ όπου } \lambda, \mu \in \mathbb{Z}, \nu \in \mathbb{N}, \text{ και μκδ}(\lambda, \mu, \nu) = 1.$$

Επειδή

$$y \nmid x \Rightarrow \frac{x}{y} \in \mathbb{Q}(\sqrt{m}) \setminus \mathfrak{O}_m,$$

έχουμε $\nu \geq 2$, όπου $\nu > 2 \Leftrightarrow$ είτε αμφότεροι οι λ, μ είναι άρτιοι είτε αμφότεροι οι λ, μ είναι περιττοί. Αρκεί (λόγω τού λήμματος 5.5.11) να αποδείξουμε ότι υπάρχουν $u, t \in \mathfrak{O}_m$, ούτως ώστε να ισχύουν οι ανισότητες (5.62). Για διευκόλυνσή μας θέτουμε

$$\nu_0 := \begin{cases} 15, & \text{όταν } m = -163, \\ 10, & \text{όταν } m = -67, \\ 8, & \text{όταν } m = -43, \\ 5, & \text{όταν } m = -19, \end{cases}$$

και διαχωρίζουμε περιπτώσεις: *Περίπτωση πρώτη*. Εάν $\boxed{\nu \geq \nu_0,}$ τότε θέτουμε

$$\mathsf{P} := \lambda a + \mu m b - \nu c, \;\; \mathsf{Q} := \lambda b + \mu a + \nu d \tag{5.63}$$

όπου $a, b, c, d \in \mathbb{Z}$, τέτοιοι ώστε $\mathsf{Q} = 1$ και $c := \left\{\frac{\lambda a + \mu m b}{\nu}\right\}_{\text{εγγ}}$. (Αυτή η επιλογή των a, b, d είναι δυνατή, διότι μκδ$(\lambda, \mu, \nu) = 1$.) Εν συνεχεία, ορίζουμε τα u, t ως ακολούθως:

$$u := a + b\sqrt{m} \in \mathfrak{O}_m, \; t := c - d\sqrt{m} \in \mathfrak{O}_m. \tag{5.64}$$

Προφανώς,

$$\frac{xu - yt}{y} = \frac{x}{y}u - t = \frac{\mathsf{P} + \mathsf{Q}\sqrt{m}}{\nu} = \frac{\mathsf{P}}{\nu} + \frac{1}{\nu}\sqrt{m}$$

και

$$\left.\begin{array}{r} (5.51) \Rightarrow \mathbf{N}(xu - yt) \geq 0, \; \mathbf{N}(y) > 0 \\ \frac{\mathbf{N}(xu-yt)}{\mathbf{N}(y)} = \mathbf{N}\left(\frac{xu-yt}{y}\right) = \mathbf{N}\left(\frac{x}{y}u - t\right) = \frac{\mathsf{P}^2 - m}{\nu^2} \\ \sqrt{m} \notin \mathbb{Q} \Rightarrow m \neq \mathsf{P}^2 \end{array}\right\} \Rightarrow \mathbf{N}\left(\frac{x}{y}u - t\right) > 0. \tag{5.65}$$

Από την άλλη μεριά,

$$\left|\frac{\mathsf{P}}{\nu}\right| = \left|\frac{\lambda a + \mu m b}{\nu} - c\right| \leq \frac{1}{2}, \tag{5.66}$$

οπότε

$$\mathbf{N}\left(\frac{x}{y}u-t\right)=\frac{\mathsf{P}^2-m}{\nu^2}\leq\frac{1}{4}-\frac{m}{\nu^2}.$$

Όταν $-m<\frac{3}{4}\nu_0^2$, τότε

$$-m<\frac{3}{4}\nu_0^2<\frac{3}{4}\nu^2\Rightarrow\mathbf{N}\left(\frac{x}{y}u-t\right)<1. \tag{5.67}$$

Τούτο είναι αληθές για τις πρώτες τρεις τιμές τού m:

$-m$	163	67	43
$\frac{3}{4}\nu_0^2$	$168,75$	75	48

Όταν $m=-19$, τότε για $\nu\geq 6$ έχουμε

$$-m=19<27=\frac{3}{4}6^2<\frac{3}{4}\nu^2\Rightarrow\mathbf{N}\left(\frac{x}{y}u-t\right)<1. \tag{5.68}$$

Για $\nu=\nu_0=5$ η (5.66) δίδει

$$\left.\begin{array}{c}|\mathsf{P}|\leq\frac{5}{2}\\ |\mathsf{P}|\in\mathbb{N}_0\end{array}\right\}\Rightarrow|\mathsf{P}|\leq 2\Rightarrow\mathsf{P}^2\leq 4\Rightarrow\mathsf{P}^2+19\leq 23<25,$$

οπότε

$$\mathbf{N}\left(\frac{x}{y}u-t\right)=\frac{\mathsf{P}^2+19}{25}<1. \tag{5.69}$$

Λόγω των (5.65), (5.67), (5.68) και (5.69) οι ανισότητες (5.62) ισχύουν για τα επιλεχθέντα u,t.

Περίπτωση δεύτερη. Εάν $\boxed{\nu=4\text{ και αμφότεροι }\lambda,\mu\text{ περιττοί,}}$ τότε

$$\exists\xi,\varrho\in\mathbb{Z}:\lambda=2\xi+1,\ \ \mu=2\varrho+1.$$

Ορίζουμε τα u,t ως ακολούθως:

$$u:=\frac{\lambda-\mu\sqrt{m}}{2}\in\mathfrak{O}_m,\ t:=\frac{\lambda^2-m\mu^2-4}{8}\in\mathfrak{O}_m.$$

Σημειωτέον ότι $t\in\mathbb{Z}$, διότι $8\mid 4\xi\left(\xi+1\right),\ 8\mid 4\varrho\left(\varrho+1\right),$

m	-163	-67	-43	-19
$-m-3$	160	64	40	16

και

$$\lambda^2-m\mu^2-4=4\xi\left(\xi+1\right)-4\varrho\left(\varrho+1\right)-m-3.$$

Επιπροσθέτως,

$$\frac{x}{y}u - t = \left(\frac{\lambda + \mu\sqrt{m}}{4}\right)\left(\frac{\lambda - \mu\sqrt{m}}{2}\right) - t = \frac{1}{2},$$

οπότε

$$0 < \mathbf{N}\left(\frac{x}{y}u - t\right) = \mathbf{N}\left(\frac{1}{2}\right) = \frac{1}{4} < 1.$$

Άρα για τα επιλεχθέντα u, t ισχύουν οι ανισότητες (5.62).

Περίπτωση τρίτη. Εάν $\boxed{\nu < \nu_0 \text{ και τουλάχιστον ένας εκ των } \lambda, \mu \text{ άρτιος για } \nu = 4,}$ τότε αξιώνουμε από τα u, t να έχουν την μορφή (5.64) και από τα P και Q να είναι βραχυγραφίες όπως στη (5.63), αλλά τούτη τη φορά με τους $a, b, d \in \mathbb{Z}$ οριζόμενους ως εξής:

$$a := \lambda, \;\; b := -\mu, \;\; d := 0$$

και τον $c \in \mathbb{Z}$ επιλεγμένον κατά τέτοιον τρόπο, ώστε

$$\frac{\lambda^2 - m\mu^2}{\nu} \geq c > \frac{\lambda^2 - m\mu^2}{\nu} - 1.$$

Προφανώς, $\mathsf{Q} = 0$, $\mathsf{P} = \lambda^2 - m\mu^2 - \nu c$ με $0 \leq \mathsf{P} < \nu$ και

$$\frac{x}{y}u - t = \frac{\mathsf{P} + \mathsf{Q}\sqrt{m}}{\nu} = \frac{\lambda^2 - m\mu^2 - \nu c}{\nu} = \frac{\lambda^2 - m\mu^2}{\nu} - c,$$

οπότε

$$\mathbf{N}\left(\frac{x}{y}u - t\right) = \frac{\mathsf{P}^2}{\nu^2} < 1.$$

Για να ισχύουν αμφότερες οι ανισότητες (5.62) για τα επιλεχθέντα u, t αρκεί, ως εκ τούτου, να αποδειχθεί ότι $\mathsf{P} \neq 0$. Τούτο έπεται από την

$$\lambda^2 - m\mu^2 \not\equiv 0 (\mathrm{mod}\, \nu). \tag{5.70}$$

Η (5.70) είναι αληθής όταν $\nu = 2$ ή $\nu = 4$ (όπου στη δεύτερη τιμή λαμβάνουμε υπ' όψιν την επιπρόσθετη προϋπόθεσή μας), διότι *είτε* ο λ είναι άρτιος και ο μ περιττός *είτε* ο λ είναι περιττός και ο μ άρτιος (αφού μκδ$(\lambda, \mu, \nu) = 1$). Η (5.70) είναι αληθής ακόμη και όταν $\nu = 8 = 2^3$, διότι τουλάχιστον ο ένας εκ των λ, μ είναι περιττός, οπότε

$$\lambda^2 - m\mu^2 \equiv \lambda^2 + 3\mu^2 \equiv \begin{cases} 4 (\mathrm{mod}\, 8), & \text{όταν } \lambda \equiv \mu \equiv 1 (\mathrm{mod}\, 2), \\ 1 (\mathrm{mod}\, 2), & \text{όταν } \lambda \equiv 1 (\mathrm{mod}\, 2),\ \mu \equiv 0 (\mathrm{mod}\, 2) \\ & \text{ή } \lambda \equiv 0 (\mathrm{mod}\, 2),\ \mu \equiv 1 (\mathrm{mod}\, 2). \end{cases}$$

Για τις εναπομείνασες περιπτώσεις, όπου το ν έχει ως διαιρέτη του κάποιον πρώτο αριθμό p, $2 < p \leq \nu < \nu_0$, η επαλήθευση τής (5.70) ανάγεται στην επαλήθευση των ακολούθων:

$$\lambda^2 - m\mu^2 \not\equiv 0(\mathrm{mod}\, p), \ \ \forall p \in \Xi,$$

όπου $\Xi := \{p |\, p \text{ πρώτος} \geq 3,\ p \mid \nu\}$. Επειδή (εξ υποθέσεως) $\nu < \nu_0$, το Ξ είναι (κατά περίπτωση) το εξής:

m	-163	-67	-43	-19
ν_0	15	10	8	5
Ξ	$\{3,5,7,11,13\}$	$\{3,5,7\}$	$\{3,5,7\}$	$\{3\}$

Θα εργασθούμε με «εις άτοπον απαγωγή». Ας υποθέσουμε ότι υπάρχει κάποιος $p \in \Xi$, τέτοιος ώστε

$$\lambda^2 - m\mu^2 \equiv 0(\mathrm{mod}\, p).$$

Εάν το p ήταν διαιρέτης τού μ, τότε θα ήταν διαιρέτης και τού λ, πράγμα αδύνατον αφού μκδ$(\lambda, \mu, \nu) = 1$. Άρα μκδ$(\mu, p) = 1$, οπότε (λόγω τής προτάσεως 3.4.1)

$$\exists \mu' \in \mathbb{Z} : \mu\mu' \equiv 1(\mathrm{mod}\, p).$$

Έστω $\kappa := \lambda\mu'$. Τότε

$$\lambda^2 - m\mu^2 \equiv 0(\mathrm{mod}\, p) \Rightarrow \left(\lambda^2 - m\mu^2\right)(\mu')^2 \equiv 0(\mathrm{mod}\, p) \Rightarrow \kappa^2 \equiv m(\mathrm{mod}\, p). \quad (5.71)$$

Αρκεί να αποδείξουμε ότι η ισοτιμία (5.71) είναι αναληθής για όλους τους δυνατούς πρώτους αριθμούς $p \geq 3$.

(i) Εάν $p = 3$, τότε $m \in \{-163, -67, -43, -19\}$ με $m \equiv 2(\mathrm{mod}\, 3)$, ενώ $\kappa^2 \equiv 0$ ή $1(\mathrm{mod}\, 3)$.

(ii) Εάν $p = 5$, τότε έχουμε $m \in \{-163, -67, -43\}$ με -163, $-43 \equiv 2(\mathrm{mod}\, 5)$ και $-67 \equiv 3(\mathrm{mod}\, 5)$, ενώ $\kappa^2 \equiv 0, 1$ ή $4(\mathrm{mod}\, 5)$.

(iii) Εάν $p = 7$, τότε $m \in \{-163, -67, -43\}$ με $-163 \equiv 5(\mathrm{mod}\, 7)$, $-67 \equiv 3(\mathrm{mod}\, 7)$ και $-43 \equiv 6(\mathrm{mod}\, 7)$, ενώ $\kappa^2 \equiv 0, 1, 4$ ή $2(\mathrm{mod}\, 7)$.

(iv) Εάν $p = 11$, τότε $m = -163 \equiv 2(\mathrm{mod}\, 11)$, ενώ $\kappa^2 \equiv 0, 1, 4, 9, 5$ ή $3(\mathrm{mod}\, 11)$.

(v) Εάν $p = 13$, τότε $m = -163 \equiv 6(\mathrm{mod}\, 13)$, ενώ $\kappa^2 \equiv 0, 1, 4, 9, 3, 12$ ή $10(\mathrm{mod}\, 13)$.

Εδώ περατούται η απόδειξη τής προτάσεως. □

5.5.13 Πόρισμα. *Εάν $m \in \{-163, -67, -43, -19\}$, τότε η $\mathfrak{O}_m$ είναι Π.Κ.Ι. αλλά δεν είναι ευκλείδεια περιοχή.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το θεώρημα 5.5.7 και την πρόταση 5.5.12. □

Η πρόταση 5.5.12 ισχυροποιείται κατά τρόπο ουσιαστικό ως ακολούθως:

5.5.14 Θεώρημα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν $m < 0$, τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η ακεραία περιοχή $\mathfrak{O}_m$ είναι Π.Κ.Ι.*

(ii) $m \in \{-163, -67, -43, -19, -11, -7, -3, -2, -1\}$.

5.5.15 Σημείωση. (i) Αριθμητικές μαρτυρίες και υπολογισμοί για το ότι οι ανωτέρω εννέα αριθμοί m είναι οι *μόνοι* «υποψήφιοι», ούτως ώστε οι αντίστοιχες ακέραιες περιοχές $\mathfrak{O}_m$ να είναι Π.Κ.Ι., εντοπίζονται ήδη στα έργα τού C.-F. Gauss και άλλων μαθηματικών τής εποχής του. Το έτος 1934 οι Heilbronn και Linfoot[26] διεπίστωσαν ότι, στην περίπτωση που θα υπήρχε αρνητικός ακέραιος m στερούμενος τετραγώνων (διαφορετικός των ανωτέρω εννέα) με αυτήν την ιδιότητα, ο $|m|$ θα όφειλε να είναι πολύ μεγάλος. Το 1952 Heegner[27] έδωσε μία απόδειξη τού αδυνάτου τής υπάρξεως τέτοιου αριθμού, η οποία όμως περιείχε ορισμένα λάθη. Οι πρώτες ορθές αποδείξεις οφείλονται στους Baker[28] και Stark[29] (στα μέσα τής δεκαετίας τού 1960). Τέλος, το 1968 οι Birch[30], Deuring[31] και Siegel[32] κατόρθωσαν να διορθώσουν ακόμη και τα λάθη τής αρχικής αποδείξεως τού Heegner.

(ii) Ένα θεώρημα ανάλογο τού 5.5.14 δεν έχει -μέχρι στιγμής- αποδειχθεί για *θετικούς* m. Ωστόσο, υπάρχουν αρκετά χρήσιμα αποτελέσματα υπολογιστικής φύσεως. Επί παραδείγματι, οι (στερούμενοι τετραγώνων) αριθμοί

$$2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29,$$
$$31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61,$$
$$62, , 67, 69, 71, 73, 77, 83, 86, 89, 93, 94 \text{ και } 97$$

είναι οι μόνοι m, $1 < m \leq 100$, για τους οποίους η $\mathfrak{O}_m$ είναι Π.Κ.Ι. Ακόμη και το *φυσικό ερώτημα* τού κατά πόσον υπάρχουν *άπειροι* θετικοί m με αυτήν την ιδιότητα δεν έχει εισέτι απαντηθεί.

5.5.16 Πόρισμα. *Έστω m ένας ακέραιος στερούμενος τετραγώνων. Εάν $m < 0$, τότε η $\mathfrak{O}_m$ είναι Π.Κ.Ι. και μη ευκλείδεια περιοχή εάν και μόνον εάν*

$$m \in \{-163, -67, -43, -19\}.$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τα θεωρήματα 5.5.7 και 5.5.14. □

[26] Heilbronn H. and Linfoot E.H.: *On the imaginary quadratic corpora of class-number one*, Quart. J. Math. (Oxford), Vol. **5**, (1934), 293-301.

[27] Heegner K.: *Diophantische Analysis und Modulfunktionen*, Math. Z. **56**, (1952), 227-253.

[28] Baker A.: *Linear forms in the logarithms of algebraic numbers*, Mathematika **13**, (1966), 204-216.

[29] Stark H.M.: *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14**, (1967), 1-27.

[30] Birch B.J.: *Diophantine analysis and modular functions*, Proc. Conf. in Algebraic Geometry, Tata Institute, Bombay, (1968), 35-42.

[31] Deuring M: *Imaginäre quadratische Zahlkörper mit Klassenzahl Eins,* Invent. Math. **5**, (1968), 169-179.

[32] Siegel C.L.: *Zum Beweise des Starkschen Satzes*, Invent. Math. **5**, (1968), 180-191.

5.6 ΠΕΡΙΟΧΕΣ ΜΟΝΟΣΗΜΑΝΤΗΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΕΩΣ

5.6.1 Ορισμός. Μια ακεραία περιοχή R καλείται **περιοχή με παραγοντοποίηση** όταν κάθε $a \in R \setminus (R^\times \cup \{0_R\})$ διαθέτει σύντροφο παριστώμενο ως γινόμενο πεπερασμένου πλήθους αναγώγων στοιχείων τής R, ήτοι όταν γράφεται υπό τη μορφή

$$a = uq_1q_2 \cdots q_k,$$

όπου $u \in R^\times$, $k \in \mathbb{N}$ και τα $q_1, q_2, \ldots, q_k$ είναι ανάγωγα στοιχεία τής R.

5.6.2 Ορισμός. Μια ακεραία περιοχή R καλείται **περιοχή μονοσήμαντης παραγοντοποιήσεως** (=: **Π.Μ.Π.**) όταν πληροί τις ακόλουθες συνθήκες:

(i) Η R είναι περιοχή με παραγοντοποίηση (υπό την έννοια τού 5.6.1) και

(ii) για οιεσδήποτε παραστάσεις

$$a \underset{\text{συν.}}{\sim} q_1q_2 \cdots q_k \underset{\text{συν.}}{\sim} q'_1q'_2 \cdots q'_l$$

συντρόφων ενός $a \in R \setminus (R^\times \cup \{0_R\})$ ως γινομένων πεπερασμένου πλήθους αναγώγων στοιχείων τής R, έχουμε $k = l$ και υπάρχει μια μετάταξη $\sigma \in \mathfrak{S}_k$ τού συνόλου $\{1, \ldots, k\}$, τέτοια ώστε να ισχύει $q_{\sigma(j)} \underset{\text{συν.}}{\sim} q'_j, \forall j \in \{1, \ldots, k\}$.

5.6.3 Θεώρημα. *Έστω R μια ακεραία περιοχή. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η R είναι Π.Μ.Π.*

(ii) *Η R είναι περιοχή με παραγοντοποίηση και κάθε στοιχείο $q \in R \setminus (R^\times \cup \{0_R\})$ είναι πρώτο εάν και μόνον εάν είναι ανάγωγο*.

(iii) *Κάθε $a \in R \setminus (R^\times \cup \{0_R\})$ διαθέτει κάποιον σύντροφο παριστώμενο ως γινόμενο πεπερασμένου πλήθους πρώτων στοιχείων τής R.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii): Λόγω τού (iii) τής προτάσεως 5.3.4 αρκεί να αποδείξουμε ότι κάθε ανάγωγο στοιχείο $r \in R \setminus (R^\times \cup \{0_R\})$ είναι πρώτο στοιχείο τής R. Ας υποθέσουμε ότι υπάρχουν $a, b \in R$, τέτοια ώστε να ισχύει $r \mid ab$. Τότε υπάρχει $c \in R$ με $ab = rc$. Γράφοντας τα a, b, c ως

$$a = uq_1q_2 \cdots q_k, \quad b = u'q'_1q'_2 \cdots q'_l, \quad c = u''q''_1q''_2 \cdots q''_m,$$

ήτοι ως συντρόφους γινομένων πεπερασμένου πλήθους αναγώγων στοιχείων τού R (όπου $u, u', u'' \in R^\times$), λαμβάνουμε

$$uu' \left(\prod_{j=1}^{k} q_j\right) \left(\prod_{\varrho=1}^{l} q'_\varrho\right) = ab = u''\, r\, q''_1q''_2 \cdots q''_m.$$

Επειδή η R είναι Π.Μ.Π., είτε υπάρχει $j \in \{1, \dots, k\}$ με $r \underset{\text{συν.}}{\sim} q_j$ είτε υπάρχει $\varrho \in \{1, \dots, l\}$ με $r \underset{\text{συν.}}{\sim} q'_\varrho$. Κατά συνέπειαν, είτε $r \mid a$ είτε $r \mid b$.

(ii)⇒(iii): Τούτο είναι προφανές.

(iii)⇒(i): Έστω τυχόν $a \in R \setminus (R^\times \cup \{0_R\})$. Εξ υποθέσεως υπάρχουν $u \in R^\times$ και πρώτα στοιχεία $p_1, \dots, p_k$, τέτοια ώστε $a = up_1p_2 \cdots p_k$. Επειδή κάθε πρώτο στοιχείο τής R είναι ανάγωγο (βλ. 5.3.4 (iii)), η R πληροί τη συνθήκη (i) τού ορισμού 5.6.2. Εάν το a διαθέτει μια δεύτερη παράσταση

$$a = wq_1q_2 \cdots q_l,$$

όπου $w \in R^\times$ και τα $q_1, \dots, q_l$ ανάγωγα στοιχεία τής R, τότε

$$\left.\begin{array}{r} p_1 \mid p_1p_2 \cdots p_k = u^{-1}wq_1q_2 \cdots q_l \\ p_1 \text{ πρώτο}, \, p_1 \nmid u^{-1}, \; p_1 \nmid w \end{array}\right\} \Longrightarrow \exists j_1 \in \{1, \dots, l\} : p_1 \mid q_{j_1}.$$

Επειδή το q_{j_1} είναι ανάγωγο και το p_1 δεν είναι αντιστρέψιμο, έχουμε $p_1 \underset{\text{συν.}}{\sim} q_{j_1}$, ήτοι $p_1 = eq_{j_1}$ για κάποιο $e \in R^\times$. Ύστερα από απλοποίηση τού p_1 στην ανωτέρω ισότητα λαμβάνουμε

$$\left.\begin{array}{r} p_2 \mid p_2 \cdots p_k = e^{-1}u^{-1}w\Big(\displaystyle\prod_{\varrho \in \{1,..,l\} \setminus \{j_1\}} q_\varrho\Big) \\ p_2 \text{ πρώτο στοιχείο}, \, p_2 \nmid e^{-1}, \; p_2 \nmid u^{-1}, \; p_2 \nmid w \end{array}\right\} \Rightarrow \exists j_2 \in \{1,..,l\} \setminus \{j_1\} : p_2 \mid q_{j_2},$$

οπότε και πάλι $p_2 \underset{\text{συν.}}{\sim} q_{j_2}$. Εφαρμόζοντας την ίδια συλλογιστική συμπεραίνουμε ότι $k \leq l$ (έπειτα από k εν συνόλω βήματα) και ότι

$$\exists \{j_1, j_2, \dots, j_k\} \subseteq \{1, \dots, l\} : p_\varrho \underset{\text{συν.}}{\sim} q_{j_\varrho}, \; \forall \varrho \in \{1, \dots, k\}.$$

Εάν ίσχυε η ανισότητα $k < l$, τότε θα είχαμε

$$\underbrace{1_R = c\,\Big(\prod_{\varrho \in \{1,..,l\} \setminus \{j_1,..,j_k\}} q_\varrho\Big), \text{ για κάποιο } c \in R^\times}_{\Downarrow}$$
$$\exists \varrho \in \{1,..,l\} \setminus \{j_1,..,j_k\} : q_\varrho \mid 1 \Longrightarrow q_\varrho \in R^\times,$$

πράγμα άτοπο. Συνεπώς, $k = l$, και ορίζοντας τη μετάταξη $\sigma \in \mathfrak{S}_k$ μέσω τού τύπου $\sigma(\varrho) = j_\varrho$ για κάθε $\varrho \in \{1, \dots, k\}$ λαμβάνουμε $p_\varrho \underset{\text{συν.}}{\sim} q_{\sigma(\varrho)}$. Άρα η R πληροί *και* τη συνθήκη (ii) τού ορισμού 5.6.2, οπότε η R είναι όντως μια Π.Μ.Π. □

5.6.4 Ορισμός. Λέμε ότι μια ακεραία περιοχή R πληροί τη **συνθήκη των αλυσίδων γνησίων διαιρετών** όταν κάθε ανιούσα αλυσίδα *κυρίων ιδεωδών*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

τής R είναι *στάσιμη*, ήτοι όταν $\exists k \in \mathbb{N}$, για τον οποίο ισχύει $I_n = I_k$ για κάθε φυσικό αριθμό $n \geq k$. Η συνθήκη αυτή ισοδυναμεί με την ακόλουθη: Δεν υπάρχει καμία (άπειρη) ακολουθία $(a_n)_{n\in\mathbb{N}}$ στοιχείων τής R, τέτοια ώστε ο a_{n+1} να είναι *γνήσιος διαιρέτης* τού a_n, για κάθε $n \in \mathbb{N}$. (Σημειωτέον ότι, λόγω των (i), (ii) και (iv) τής προτάσεως 5.2.4 και τού ορισμού των γνησίων διαιρετών (βλ. 5.2.8), ο $b \in R$ είναι ένας γνήσιος διαιρέτης ενός $a \in R$ εάν και μόνον εάν $\langle a\rangle \subsetneqq \langle b\rangle \subsetneqq R$)

5.6.5 Θεώρημα. *Έστω R μια ακεραία περιοχή. Εάν υποθέσουμε ότι η R πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών, τότε η R είναι περιοχή με παραγοντοποίηση.*

ΑΠΟΔΕΙΞΗ. Έστω

$$\Lambda := \left\{ a \in R \diagdown \left(R^{\times} \cup \{0_R\}\right) \;\middle|\; \begin{array}{c} \nexists c \underset{\text{συν.}}{\sim} a \text{ παριστώμενος} \\ \text{ως γινόμενο πεπερασμένου πλήθους} \\ \text{αναγώγων στοιχείων τής } R. \end{array} \right\}.$$

Ας υποθέσουμε ότι η R πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών, ότι $\Lambda \neq \varnothing$ κι ας θέσουμε για κάθε $a \in \Lambda$,

$$\Gamma_a := \{\, b \in \Lambda \mid b \text{ είναι γνήσιος διαιρέτης τού } a\}\,.$$

Τότε $\Gamma_a \neq \varnothing$ για οιοδήποτε $a \in \Lambda$. (Πράγματι· εάν υπήρχε $a \in \Lambda$, για το οποίο θα είχαμε $\Gamma_a = \varnothing$, τότε το ίδιο το a θα όφειλε να είναι ανάγωγο, κάτι που θα αντέκειτο προς την υπόθεσή μας.) Σύμφωνα με το αξίωμα τής επιλογής,

$$(\Gamma_a \neq \varnothing,\ \forall a \in \Lambda) \Longrightarrow \prod_{a\in\Lambda} \Gamma_a \neq \varnothing,$$

οπότε υπάρχει μια απεικόνιση

$$f : \Lambda \longrightarrow \bigcup_{a\in\Lambda} \Gamma_a, \quad \text{με } f(a) \in \Gamma_a,\ \forall a \in \Lambda,$$

ήτοι τέτοια, ώστε η εικόνα $f(a)$ τού a μέσω τής f να είναι γνήσιος διαιρέτης τού $a, \forall a \in \Lambda$. Επιλέγοντας ένα τυχόν στοιχείο τού Λ και ονομάζοντάς το a_1 έχουμε τη δυνατότητα να ορίσουμε μια αναδρομική απεικόνιση $\mathfrak{K} : \mathbb{N} \longrightarrow \Lambda$ μέσω των τύπων

$$\mathfrak{K}(1) := a_1, \qquad \mathfrak{K}(n+1) := f(\mathfrak{K}(n)) =: a_{n+1}, \ \ \forall n \in \mathbb{N}.$$

Η κατ' αυτόν τον τρόπο σχηματιζομένη ακολουθία $(a_n)_{n\in\mathbb{N}}$ στοιχείων τής R είναι τέτοια, ώστε ο a_{n+1} να είναι *γνήσιος διαιρέτης* τού a_n, για κάθε $n \in \mathbb{N}$. Ως εκ τούτου, η R δεν μπορεί να πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών, κάτι που αντιφάσκει προς την υπόθεσή μας! Άρα τελικώς $\Lambda = \varnothing$ και η R είναι πράγματι περιοχή με παραγοντοποίηση. □

5.6.6 Πόρισμα. *Κάθε ναιτεριανή περιοχή είναι περιοχή με παραγοντοποίηση.*

ΑΠΟΔΕΙΞΗ. Κάθε ναιτεριανή περιοχή πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών (διότι πληροί τη συνθήκη των ανιουσών αλυσίδων επί τού συνόλου *όλων* των ιδεωδών της) και είναι, ως εκ τούτου, περιοχή με παραγοντοποίηση (λόγω τού θεωρήματος 5.6.5). □

5.6.7 Παραδείγματα. (i) Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Τότε η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{m}]$, ούσα ναιτεριανή (βλ. πρόταση 4.1.13), είναι περιοχή με παραγοντοποίηση. Ωστόσο, όταν $m \equiv 1 (\mathrm{mod}\, 4)$ ή $m \leq -3$, η $\mathbb{Z}[\sqrt{m}]$ *δεν είναι* Π.Μ.Π.! (Βλ. 5.3.8 (i) και (ii), και 5.6.3 (i)⇒(ii).)

(ii) Υποδακτύλιοι περιοχών μονοσήμαντης παραγοντοποιήσεως δεν είναι απαραιτήτως Π.Μ.Π. Επί παραδείγματι, η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{-3}]$ δεν είναι Π.Μ.Π., αλλά αποτελεί υποπεριοχή τής $\mathfrak{O}_{-3}$ (που είναι Π.Μ.Π.).

5.6.8 Πόρισμα. *Κάθε Π.Κ.Ι. είναι Π.Μ.Π.*

ΑΠΟΔΕΙΞΗ. Έστω R τυχούσα Π.Κ.Ι. Επειδή η R είναι ναιτεριανή, κάθε στοιχείο $a \in R \setminus (R^\times \cup \{0_R\})$ διαθέτει σύντροφο παριστώμενο ως γινόμενο πεπερασμένου πλήθους αναγώγων στοιχείων τής R (βάσει τού πορίσματος 5.6.6). Χρησιμοποιώντας τό γεγονός τού ότι κάθε ανάγωγο στοιχείο μιας Π.Κ.Ι. είναι πρώτο, καθώς και την ισοδυναμία των (i) και (iii) τού θεωρήματος 5.6.3, συμπεραίνουμε ότι η R οφείλει να είναι περιοχή μονοσήμαντης παραγοντοποιήσεως. □

5.6.9 Σημείωση. Το αντίστροφο τού πορίσματος 5.6.8 δεν είναι πάντοτε αληθές. Επί παραδείγματι, ο πολυωνυμικός δακτύλιος $\mathbb{Z}[\mathrm{X}]$ είναι Π.Μ.Π. αλλά δεν είναι Π.Κ.Ι. (Βλ. εδ. 5.10.15 (i).) Από την άλλη μεριά, είναι αξιοσημείωτο ότι το αντίστροφο ισχύει *για όλες* τις ακέραιες περιοχές $\mathfrak{O}_m$.

5.6.10 Θεώρημα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Τότε η ακεραία περιοχή $\mathfrak{O}_m$ είναι Π.Μ.Π. εάν και μόνον εάν είναι Π.Κ.Ι.*

ΑΠΟΔΕΙΞΗ. Βλ. H. Lüneburg: *Vorlesungen über Zahlentheorie*, Birkhäuser Verlag, 1978, Satz 130, σελ. 90-91. □

5.6.11 Ορισμός. Έστω R μια Π.Μ.Π. και έστω $r \in R \setminus \{0_R\}$. Τότε το r είτε είναι αντιστρέψιμο είτε γράφεται ως

$$r = w s_1 s_2 \cdots s_k,$$

όπου $w \in R^\times$, $k \in \mathbb{N}$ και τα $s_1, s_2, \ldots, s_k$ πρώτα (= ανάγωγα) στοιχεία τής R. Εάν $s_1 \underset{\text{συν.}}{\sim} s_2 \underset{\text{συν.}}{\sim} \cdots \underset{\text{συν.}}{\sim} s_k =: p$, τότε $r = up^k$, για κάποιο $u \in R^\times$. Ειδάλλως, για να συμπτύξουμε σε αυτό το γινόμενο όσα εκ των $s_1, s_2, \ldots, s_k$ είναι ανά δύο συντροφικά (με την εισαγωγή «δυνάμεων») μπορούμε (πιθανώς ύστερα από μια αναδιάταξη δεικτών) να υποθέσουμε ότι

$$s_1 \underset{\text{συν.}}{\sim} \cdots \underset{\text{συν.}}{\sim} s_{j_1}, s_{j_1+1} \underset{\text{συν.}}{\sim} \cdots \underset{\text{συν.}}{\sim} s_{j_2}, s_{j_2+1} \underset{\text{συν.}}{\sim} \cdots \underset{\text{συν.}}{\sim} s_{j_3} \cdots\cdots, s_{j_{\ell-1}+1} \underset{\text{συν.}}{\sim} \cdots \underset{\text{συν.}}{\sim} s_{j_\ell} = s_k$$

για κατάλληλα $\{j_1, j_2, \dots, j_\ell\} \subseteq \{1, \dots, k\},\ 2 \le l \le k$, με

$$1 = j_1 < j_2 < \cdots < j_{\ell-1} < j_\ell = k$$

και $s_{j_\mu} \underset{\text{συν.}}{\not\sim} s_{j_{\mu'}}$ για οιουσδήποτε $\mu, \mu' \in \{1, \dots, \ell\}, \mu \neq \mu'$. Θέτοντας

$$\nu_1 := j_1,\ \nu_2 := j_2 - j_1,\ \dots,\ \nu_\ell := j_\ell - j_{\ell-1}, \quad p_\mu := s_{j_\mu},\ \forall \mu \in \{1, \dots, \ell\},$$

και λαμβάνοντας υπ' όψιν ότι $s_{\rho_\mu} = u_{\rho_\mu} s_{j_\mu}$ για κάποιο $u_{\rho_\mu} \in R^\times$ και για οιουσδήποτε δείκτες $\rho_\mu \in \{1, ..., j_\mu\}, \mu \in \{1, \dots, \ell\}$, το r γράφεται ως

$$\boxed{r = u p_1^{\nu_1} p_2^{\nu_2} \cdots p_\ell^{\nu_\ell},} \tag{5.72}$$

όπου $u := w(\prod_{\mu=1}^{\ell}(\prod_{\rho_\mu=1}^{j_\mu} u_{\rho_\mu})) \in R^\times$. Η έκφραση (5.72) καλείται **παράσταση τού r ως γινομένου πρώτων στοιχείων** ή **αποσύνθεση τού r σε γινόμενο πρώτων στοιχείων**. Το r μπορεί να γραφεί υπό μία ακόμη πιο βολική μορφή στην οποία *συμπεριλαμβάνεται και η περίπτωση κατά την οποία* $r \in R^\times$, ως ακολούθως: Το σύνολο των πρώτων (= αναγώγων) στοιχείων τής R αποσυντίθεται σε κλάσεις ισοδυναμίας ως προς τη σχέση "$\underset{\text{συν.}}{\sim}$", ήτοι σε σαφώς διακεκριμένες κλάσεις συντροφικών πρώτων στοιχείων. Έστω $\mathcal{P}_R$ ένα *πλήρες σύστημα εκπροσώπων* αυτών των κλάσεων ισοδυναμίας (ήτοι ένα υποσύνολο τού συνόλου των πρώτων στοιχείων τής R, το οποίο περιέχει *ακριβώς ένα* στοιχείο από καθεμιά εξ αυτών). Τότε

$$\boxed{r = u \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(r)},\ \ u \in R^\times,} \tag{5.73}$$

όπου

$$\boldsymbol{\nu}_p(r) := \begin{cases} \max\left\{k \in \mathbb{N} : p^k \mid r\right\}, & \text{όταν } p \mid r, \\ 0, & \text{όταν } p \nmid r. \end{cases}$$

5.6.12 Πρόταση. *Έστω R μια Π.Μ.Π. Εάν $r, s \in R \setminus \{0_R\}$, τότε ισχύουν τα ακόλουθα*:

(i) $\boldsymbol{\nu}_p(rs) = \boldsymbol{\nu}_p(r) + \boldsymbol{\nu}_p(s),\ \forall p \in \mathcal{P}_R$.

(ii) $r \mid s \iff \boldsymbol{\nu}_p(r) \le \boldsymbol{\nu}_p(s),\ \forall p \in \mathcal{P}_R$.

(iii) $r \underset{\text{συν.}}{\sim} s \iff \boldsymbol{\nu}_p(r) = \boldsymbol{\nu}_p(s),\ \forall p \in \mathcal{P}_R$.

(iv) $r \in R^\times \iff \boldsymbol{\nu}_p(r) = 0,\ \forall p \in \mathcal{P}_R$.

(v) *Εάν* $r + s \neq 0_R$, *τότε* $\boldsymbol{\nu}_p(r+s) \ge \min\{\boldsymbol{\nu}_p(r), \boldsymbol{\nu}_p(s)\},\ \forall p \in \mathcal{P}_R$.

(vi) *Εάν* $\boldsymbol{\nu}_p(r) < \boldsymbol{\nu}_p(s)$ *για κάποιο* $p \in \mathcal{P}_R$, *τότε* $\boldsymbol{\nu}_p(r+s) = \boldsymbol{\nu}_p(r)$.

ΑΠΟΔΕΙΞΗ. (i) Εάν οι

$$r = u \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(r)},\ \ s = w \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(s)}, \tag{5.74}$$

είναι οι παραστάσεις των r και s ως γινομένων πρώτων στοιχείων, τότε, λόγω τού μονοσημάντου τής παραστάσεως τού rs, έχουμε

$$rs = uw \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(r)+\boldsymbol{\nu}_p(s)} \Longrightarrow \boldsymbol{\nu}_p(rs) = \boldsymbol{\nu}_p(r) + \boldsymbol{\nu}_p(s),\ \forall p \in \mathcal{P}_R.$$

(ii) Εάν $r \mid s$, τότε $\exists r' \in R : s = rr'$, οπότε

$$\left.\begin{array}{r} \text{(i)} \Rightarrow \boldsymbol{\nu}_p(s) = \boldsymbol{\nu}_p(rr') = \boldsymbol{\nu}_p(r) + \boldsymbol{\nu}_p(r'),\ \forall p \in \mathcal{P}_R \\ \boldsymbol{\nu}_p(r') \geq 0,\ \forall p \in \mathcal{P}_R \end{array}\right\} \Rightarrow \boldsymbol{\nu}_p(s) \geq \boldsymbol{\nu}_p(r),\ \forall p \in \mathcal{P}_R.$$

(iii) Αυτό έπεται άμεσα από το (ii).

(iv) Εάν $r \in R^\times$, τότε $r \underset{\text{συν.}}{\sim} 1$, οπότε εφαρμόζοντας το (iii) λαμβάνουμε

$$\boldsymbol{\nu}_p(r) = \boldsymbol{\nu}_p(1) = 0,\ \forall p \in \mathcal{P}_R.$$

Το αντίστροφο είναι προφανές.

(v) Εάν υποθέσουμε ότι $r + s \neq 0_R, \mu_p := \min\{\boldsymbol{\nu}_p(r), \boldsymbol{\nu}_p(s)\}$ και ότι οι (5.74) είναι οι οι παραστάσεις των r και s ως γινομένων πρώτων στοιχείων, τότε

$$r + s = \prod_{p\in\mathcal{P}_R} p^{\mu_p} \left(u \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(r)-\mu_p} + w \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(s)-\mu_p} \right),$$

οπότε $\boldsymbol{\nu}_p(r + s) \geq \mu_p,\ \forall p \in \mathcal{P}_R$.

(vi) Ας διατηρήσουμε τους συμβολισμούς τους εισαχθέντες στο (v). Εάν ισχύει η ανισότητα $\boldsymbol{\nu}_p(r) < \boldsymbol{\nu}_p(s)$ για κάποιο $p \in \mathcal{P}_R$, τότε $\mu_p = \boldsymbol{\nu}_p(r)$, πράγμα που σημαίνει ότι

$$p \nmid u \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(r)-\mu_p}, \quad p \mid w \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(s)-\mu_p}.$$

Άρα $\boldsymbol{\nu}_p(r + s) = \boldsymbol{\nu}_p(r)$. □

5.6.13 Θεώρημα. *Εάν μια ακεραία περιοχή R είναι Π.Μ.Π., τότε η R είναι περιοχή με μ.κ.δ. Επιπροσθέτως, εάν $n \in \mathbb{N},\ n \geq 2$, και $a_1, a_2, \ldots, a_n \in R \setminus \{0_R\}$,τότε*

$$\boxed{\prod_{p\in\mathcal{P}_R} p^{\min\{\boldsymbol{\nu}_p(a_1),\boldsymbol{\nu}_p(a_2),\ldots,\boldsymbol{\nu}_p(a_n)\}} \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)} \tag{5.75}$$

και

$$\boxed{\prod_{p\in\mathcal{P}_R} p^{\max\{\boldsymbol{\nu}_p(a_1),\boldsymbol{\nu}_p(a_2),\ldots,\boldsymbol{\nu}_p(a_n)\}} \in \text{ΕΚΠ}_R(a_1, \ldots, a_n)} \tag{5.76}$$

ΑΠΟΔΕΙΞΗ. Εάν οι

$$a_j = u_j \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(a_j)},\ \ u_j \in R^\times,\ \ j \in \{1,\dots,n\},$$

είναι οι παραστάσεις (5.73) των $a_1,\dots,a_n$ ως γινομένων πρώτων στοιχείων, τότε $a_j \underset{\text{συν.}}{\sim} \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(a_j)}$. Έστω c ένα στοιχείο τής R, για το οποίο ισχύει $c \mid a_j$ για κάθε $j \in \{1,\dots,n\}$. Λαμβάνοντας υπ' όψιν το (ii) τής προτάσεως 5.6.12, για κάθε $j \in \{1,\dots,n\}$ έχουμε

$$\boldsymbol{\nu}_p(c) \le \boldsymbol{\nu}_p(a_j) \Longrightarrow \boldsymbol{\nu}_p(c) \le \min\left\{\boldsymbol{\nu}_p(a_1),\dots,\boldsymbol{\nu}_p(a_n)\right\},\ \forall p \in \mathcal{P}_R.$$

Κατά συνέπειαν, το

$$d := \prod_{p\in\mathcal{P}_R} p^{\min\{\boldsymbol{\nu}_p(a_1),\boldsymbol{\nu}_p(a_2),\dots,\boldsymbol{\nu}_p(a_n)\}}$$

είναι διαιρέτης τού a_j για κάθε $j \in \{1,\dots,n\}$ και $d \mid c$. Ως εκ τούτου, το d είναι ένας μέγιστος κοινός διαιρέτης των $a_1,\dots,a_n$ και το (5.75) είναι αληθές. Εν συνεχεία, υποθέτουμε ότι το c είναι ένα στοιχείο τής R, για το οποίο ισχύει $a_j \mid c$ για κάθε $j \in \{1,\dots,n\}$. Λαμβάνοντας εκ νέου υπ' όψιν το (ii) τής προτάσεως 5.6.12, για κάθε $j \in \{1,\dots,n\}$ έχουμε

$$\boldsymbol{\nu}_p(c) \ge \boldsymbol{\nu}_p(a_j) \Longrightarrow \boldsymbol{\nu}_p(c) \ge \max\left\{\boldsymbol{\nu}_p(a_1),\dots,\boldsymbol{\nu}_p(a_n)\right\},\ \forall p \in \mathcal{P}_R.$$

Κατά συνέπειαν, τα a_j είναι διαιρέτες τού

$$t := \prod_{p\in\mathcal{P}_R} p^{\max\{\boldsymbol{\nu}_p(a_1),\boldsymbol{\nu}_p(a_2),\dots,\boldsymbol{\nu}_p(a_n)\}}$$

για κάθε $j \in \{1,\dots,n\}$ και $c \mid t$. Ως εκ τούτου, το t είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1,\dots,a_n$ και το (5.76) είναι αληθές. □

5.6.14 Πόρισμα. *Εάν R είναι μια Π.Μ.Π. και $a,b \in R$, τότε*

$$\boxed{dt \underset{\text{συν.}}{\sim} ab,\ \ \forall d \in \text{ΜΚΔ}_R(a,b) \text{ και } \forall t \in \text{ΕΚΠ}_R(a,b).} \tag{5.77}$$

ΑΠΟΔΕΙΞΗ. Εάν τουλάχιστον ένα εκ των a,b είναι $= 0_R$, τότε το (5.77) είναι προφανές. Εάν $a,b \in R\setminus\{0_R\}$, $d \in \text{ΜΚΔ}_R(a,b)$ και $t \in \text{ΕΚΠ}_R(a,b)$, τότε από τις προτάσεις 5.2.12, 5.2.23 και από το θεώρημα 5.6.13 έπεται ότι

$$d \underset{\text{συν.}}{\sim} \prod_{p\in\mathcal{P}_R} p^{\min\{\boldsymbol{\nu}_p(a),\boldsymbol{\nu}_p(b)\}},\quad t \underset{\text{συν.}}{\sim} \prod_{p\in\mathcal{P}_R} p^{\max\{\boldsymbol{\nu}_p(a),\boldsymbol{\nu}_p(b)\}}.$$

Χρησιμοποιώντας τήν ισότητα

$$\min\left\{\boldsymbol{\nu}_p(a),\boldsymbol{\nu}_p(b)\right\} + \max\left\{\boldsymbol{\nu}_p(a),\boldsymbol{\nu}_p(b)\right\} = \boldsymbol{\nu}_p(a) + \boldsymbol{\nu}_p(b),\ \forall p \in \mathcal{P}_R,$$

το (i) τής προτάσεως 5.6.12 και όσα προναφέραμε στην 5.2.7, λαμβάνουμε

$$dt \underset{\text{συν.}}{\sim} \left(\prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(a)}\right)\left(\prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(b)}\right) = \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(a)+\boldsymbol{\nu}_p(b)} = \prod_{p\in\mathcal{P}_R} p^{\boldsymbol{\nu}_p(ab)} \underset{\text{συν.}}{\sim} ab,$$

οπότε το (5.77) είναι αληθές. □

5.6.15 Πόρισμα. *Έστω R μια Π.Μ.Π. Εάν $x, y \in R\setminus(R^\times \cup \{0_R\})$ είναι σχετικώς πρώτα στοιχεία* (βλ. 5.2.16) *και $xy = z^n$, για κάποιο $z \in R\setminus\{0_R\}$ και κάποιον $n \in \mathbb{N}$, τότε ισχύουν τα εξής*:

(i) *Υπάρχουν $r, s \in R\setminus(R^\times \cup \{0_R\})$ και $u_1, u_2 \in R^\times$ με*

$$\boxed{x = u_1 r^n \text{ και } y = u_2 s^n.}$$

(ii) *Εάν κάθε αντιστρέψιμο στοιχείο τής R ισούται με την n-οστή δύναμη κάποιου (κατ' ανάγκην αντιστρεψίμου) στοιχείου τής R, τότε $\exists t, w \in R\setminus(R^\times \cup \{0_R\})$ με*

$$\boxed{x = t^n \text{ και } y = w^n.}$$

ΑΠΟΔΕΙΞΗ. (i) Επειδή $xy = z^n$, το (i) τής προτάσεως 5.6.12 δίδει

$$\boldsymbol{\nu}_p(x) + \boldsymbol{\nu}_p(y) = \boldsymbol{\nu}_p(xy) = \boldsymbol{\nu}_p(z^n) = n\boldsymbol{\nu}_p(z),\ \forall p \in \mathcal{P}_R. \tag{5.78}$$

Επειδή (κατά το θεώρημα 5.6.13 και κατά την υπόθεσή μας)

$$\left.\begin{aligned}\prod_{p\in\mathcal{P}_R} p^{\min\{\boldsymbol{\nu}_p(x),\boldsymbol{\nu}_p(y)\}} &\in \text{ΜΚΔ}_R(x,y)\\ 1_R &\in \text{ΜΚΔ}_R(x,y)\end{aligned}\right\} \underset{\text{5.2.12}}{\Longrightarrow} \prod_{p\in\mathcal{P}_R} p^{\min\{\boldsymbol{\nu}_p(x),\boldsymbol{\nu}_p(y)\}} \underset{\text{συν.}}{\sim} 1_R,$$

$$\Rightarrow \min\{\boldsymbol{\nu}_p(x), \boldsymbol{\nu}_p(y)\} \underset{\text{5.6.12 (iii)}}{=} \boldsymbol{\nu}_p(1_R) \underset{\text{5.6.12 (iv)}}{=} 0 \Rightarrow [\text{είτε } \boldsymbol{\nu}_p(x) = 0 \text{ είτε } \boldsymbol{\nu}_p(y) = 0],$$

από την (5.78) έπεται ότι

$$[n \mid \boldsymbol{\nu}_p(x) \text{ και } n \mid \boldsymbol{\nu}_p(y)],\ \forall p \in \mathcal{P}_R.$$

Θέτοντας

$$r := \prod_{p\in\mathcal{P}_R} p^{\frac{\boldsymbol{\nu}_p(x)}{n}} = \prod_{\{p\in\mathcal{P}_R:\boldsymbol{\nu}_p(y)=0\}} p^{\frac{\boldsymbol{\nu}_p(x)}{n}}$$

και

$$s := \prod_{p\in\mathcal{P}_R} p^{\frac{\boldsymbol{\nu}_p(y)}{n}} = \prod_{\{p\in\mathcal{P}_R:\boldsymbol{\nu}_p(x)=0\}} p^{\frac{\boldsymbol{\nu}_p(y)}{n}},$$

παρατηρούμε ότι

$$\left[\boldsymbol{\nu}_p(r^n) = n\boldsymbol{\nu}_p(r) = n\tfrac{\boldsymbol{\nu}_p(x)}{n} = \boldsymbol{\nu}_p(x),\ \forall p \in \mathcal{P}_R\right] \underset{\text{5.6.12 (iii)}}{\Longrightarrow} x \underset{\text{συν.}}{\sim} r^n$$

και κατ' αναλογίαν $y \underset{\text{συν.}}{\sim} s^n$. Άρα υπάρχουν $u_1, u_2 \in R^\times$ με $x = u_1 r^n$ και $y = u_2 s^n$. (Βλ. πόρισμα 5.2.5.)

(ii) Εξ υποθέσεως, $u_1 = \varepsilon_1^n$ και $u_2 = \varepsilon_2^n$ για κάποια $\varepsilon_1, \varepsilon_2 \in R^\times$. Αρκεί λοιπόν να θέσουμε $t := \varepsilon_1 r$ και $w := \varepsilon_2 s$. □

5.6.16 Θεώρημα. *Έστω R μια ακεραία περιοχή. Τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η R είναι Π.Μ.Π.*

(ii) *Η R είναι περιοχή με μ.κ.δ. και πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν η R είναι Π.Μ.Π, τότε η R είναι περιοχή με μ.κ.δ. δυνάμει τού θεωρήματος 5.6.13. Ας υποθέσουμε ότι η R δεν πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών. Τότε υπάρχει μια (άπειρη) ακολουθία $(a_n)_{n\in\mathbb{N}}$ στοιχείων τής R, τέτοια ώστε ο a_{n+1} να είναι *γνήσιος διαιρέτης* τού a_n, για κάθε $n \in \mathbb{N}$, οπότε η ανιούσα αλυσίδα κυρίων ιδεωδών

$$\langle a_1\rangle \subsetneqq \langle a_2\rangle \subsetneqq \cdots \subsetneqq \langle a_n\rangle \subsetneqq \langle a_{n+1}\rangle \subsetneqq \cdots$$

είναι μη στάσιμη. Ιδιαιτέρως, το a_n είναι γνήσιος διαιρέτης τού a_1 για κάθε $n \in \mathbb{N}$, οπότε υπάρχουν *άπειροι* γνήσιοι διαιρέτες τού a_1. Τούτο όμως είναι κάτι το *άτοπο*, διότι το $a_1 \in R \setminus (R^\times \cup \{0_R\})$ διαθέτει ως σύντροφο κάποιον

$$a \underset{\text{συν.}}{\sim} p_1^{\nu_1} p_2^{\nu_2} \cdots p_\ell^{\nu_\ell},$$

όπου $p_1, \ldots, p_\ell$ είναι ανά δύο μη συντροφικά πρώτα στοιχεία και $\nu_1, ..., \nu_\ell \in \mathbb{N}_0$, ο οποίος έχει παράγοντες *μονοσημάντως ορισμένους* (με μόνη εξαίρεση την αντικατάστασή τους από ισαρίθμους συντρόφους τους). Ως εκ τούτου, οι μόνοι γνήσιοι διαιρέτες τού a_1 είναι τα στοιχεία τού συνόλου

$$\left\{ p_1^{\mu_1} p_2^{\mu_2} \cdots p_\ell^{\mu_\ell} \;\middle|\; (\mu_1, \ldots, \mu_\ell) \in \left(\prod_{j=1}^{\ell} \{0, 1, ..., \nu_j\} \right) \setminus \{(0, ..., 0), (\nu_1, ..., \nu_\ell)\} \right\}$$

που έχει *πεπερασμένο* πληθικό αριθμό (ίσον με $(\prod_{j=1}^{\ell} (\nu_j + 1)) - 2$). Άρα τελικώς η R οφείλει να πληροί *και* τη συνθήκη των αλυσίδων γνησίων διαιρετών.

(ii)⇒(i) Επειδή η R είναι περιοχή με μ.κ.δ., κάθε ανάγωγο στοιχείο τής R είναι πρώτο (βάσει τής προτάσεως 5.3.6). Επειδή η R πληροί και τη συνθήκη των αλυσίδων γνησίων διαιρετών, είναι, επιπροσθέτως, και περιοχή με παραγοντοποίηση (κατά το θεώρημα 5.6.5). Ως εκ τούτου, η R είναι Π.Μ.Π. βάσει τής ισοδυναμίας (ii)⇔(i) τού θεωρήματος 5.6.3. □

5.7 ΑΡΙΘΜΟΘΕΩΡΗΤΙΚΕΣ ΕΦΑΡΜΟΓΕΣ Ι: ΑΘΡΟΙΣΜΑΤΑ ΤΕΤΡΑΓΩΝΩΝ

• Ερώτημα: Ποιος είναι ο *ελάχιστος* φυσικός αριθμός $k \geq 2$, ούτως ώστε *κάθε* $n \in \mathbb{N}$ να γράφεται ως άθροισμα

$$\boxed{n = x_1^2 + x_2^2 + \cdots + x_k^2}$$

τετραγώνων k ακεραίων αριθμών $x_1, x_2, ..., x_k$; Είναι προφανές ότι $k \neq 2$ και $k \neq 3$, διότι, π.χ., το 3 δεν γράφεται ως άθροισμα δύο τετραγώνων και το 7 δεν γράφεται ως άθροισμα τριών τετραγώνων ακεραίων αριθμών. Η απάντηση είναι $k = 4$: *Κάθε φυσικός αριθμός μπορεί πάντοτε να παρασταθεί ως άθροισμα τεσσάρων τετραγώνων*. (Βλ. θεώρημα 5.7.53.) Τούτο διατυπώθηκε ως εικασία το 1621 από τον C.G. Bachet (1581-1638), αν και υπάρχουν βάσιμες ενδείξεις ότι θεωρείτο ως «γνωστό» ή ως κάτι το «φυσιολογικό» ήδη από τον ίδιον τον Διόφαντο[33]. Η πρώτη του απόδειξη (περί το έτος 1770) οφείλεται στον J.-L. Lagrange (1736-1813). Εδώ θα δοθεί μια *δακτυλιοθεωρητική* απόδειξη η οποία στηρίζεται σε *πολύ απλές ιδιότητες* τού δακτυλίου $\mathrm{Mat}_{2\times 2}(\mathbb{Z}[i])$ των 2×2-πινάκων με τις εγγραφές τους ειλημμένες από τον δακτύλιο των γκαουσιανών ακεραίων. Προτού όμως προχωρήσουμε σε αυτήν, θα απαντήσουμε, μεταξύ άλλων, και στο φυσικώς εγειρόμενο, συναφές:

• Ερώτημα: *Υπό ποίες* (ικανές και αναγκαίες) *συνθήκες* γράφεται ένας $n \in \mathbb{N}$ ως άθροισμα τετραγώνων *δύο* ή *τριών* ακεραίων αριθμών;

Η απάντηση για την παράσταση ενός $n \in \mathbb{N}$ ως αθροίσματος *δύο* τετραγώνων δίδεται μέσω τού θεωρήματος 5.7.8. Για την απόδειξή του μπορεί κανείς να εκμεταλλευθεί το γεγονός ότι ο $\mathbb{Z}[i]$ είναι Π.Μ.Π. Μάλιστα, η μετάβαση και σε άλλες γνωστές επεκτάσεις τού $\mathbb{Z}$ που είναι Π.Μ.Π. μας επιτρέπει τον προσδιορισμό των πρώτων αριθμών που είναι παραστάσιμοι μέσω αρκετών ενδιαφερουσών δυαδικών ακεραίων τετραγωνικών μορφών. (Βλ. θεώρημα 5.7.31.) Τέλος, η απάντηση για το πότε ένας $n \in \mathbb{N}$ είναι παραστάσιμος ως άθροισμα *τριών* τετραγώνων δίδεται μέσω τού θεωρήματος 5.7.49 τού A.M. Legendre.

► **Αθροίσματα δύο τετραγώνων**. Αρχικώς αποδεικνύουμε το λεγόμενο *θεώρημα τού Wilson*.

5.7.1 Θεώρημα. (Wilson) *Ένας ακέραιος $p > 1$ είναι πρώτος εάν και μόνον εάν*

$$\boxed{(p-1)! \equiv -1 (\mathrm{mod}\ p).} \tag{5.79}$$

[33] Βλ. Ε. Σταμάτη: *Διοφάντου Αριθμητικά* (αρχαίο κείμενο, μετάφραση και επεξηγήσεις), Ο.Ε.Δ.Β., 1963, κεφ. V.

ΑΠΟΔΕΙΞΗ[34]. Έστω p ένας πρώτος αριθμός. Εάν $p = 2$ ή $p = 3$, τότε η (5.79) είναι προφανώς αληθής. Εάν ο p είναι πρώτος ≥ 5, θεωρούμε ένα $a \in \{1, 2, \dots, p-1\}$ και τη γραμμική ισοτιμία $ax \equiv 1 \pmod{p}$. Επειδή μκδ$(a, p) = 1$, η εν λόγω ισοτιμία έχει μοναδική λύση κατά μόδιο p, οπότε υπάρχει μονοσημάντως ορισμένος ακέραιος a', για τον οποίο ισχύει $0 \leq a' \leq p-1$ και $aa' \equiv 1 \pmod{p}$. Επειδή ο p είναι πρώτος, έχουμε

$$a = a' \Longleftrightarrow (\text{είτε } a = 1 \text{ είτε } a = p-1). \tag{5.80}$$

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 (5.80), αφού έχουμε $1 \leq a \leq p-1$ και $1 \leq a' \leq p-1$. Και αντιστρόφως· εάν $a = 1$, τότε

$$\left.\begin{array}{r} a' \equiv 1 (\mathrm{mod}\ p) \Rightarrow p \mid a'-1 \\ 1 \leq a' \leq p-1 \end{array}\right\} \Rightarrow a'-1 = 0 \Rightarrow a' = 1,$$

και εάν $a = p-1$, τότε $(p-1)\, a' \equiv 1 (\mathrm{mod}\, p) \Longrightarrow pa' \equiv a'+1 (\mathrm{mod}\, p)$, οπότε

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

και, ως εκ τούτου,

$$\left.\begin{array}{r} p \equiv a'+1 (\mathrm{mod}\ p) \Rightarrow p \mid p-(a'+1) \\ 0 \leq p-(a'+1) \leq p-2 \end{array}\right\} \Rightarrow a' = p-1,$$

και η συνεπαγωγή "$\Leftarrow$ " τής (5.80) είναι όντως αληθής. Ομαδοποιούμε, εν συνεχεία, τους εναπομένοντες φυσικούς αριθμούς

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

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

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

[34] 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 (5.79). 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.

Επειδή $p-1 \equiv -1(\mathrm{mod}\, p)$, η (5.79) προκύπτει από τη μεταβατικότητα τής σχέσεως ισοτιμίας κατά μόδιο p.

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

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

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. □

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

$$\boxed{\left(\tfrac{p-1}{2}!\right)^2 \equiv \begin{cases} -1(\mathrm{mod}\ p), & \text{όταν } p \equiv 1(\mathrm{mod}\ 4), \\ \\ 1(\mathrm{mod}\ p), & \text{όταν } p \equiv 3(\mathrm{mod}\ 4). \end{cases}}$$

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

$$\tfrac{p-1}{2} = 2k \Rightarrow \tfrac{p-1}{2}! = 1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2} = (-1)\,(-2) \cdot \ldots \cdot \left(-\tfrac{p-1}{2}\right) \tag{5.81}$$

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

$$\left.\begin{array}{l} -1 \equiv (p-1)(\mathrm{mod}\, p) \\ -2 \equiv (p-2)(\mathrm{mod}\, p) \\ \qquad \vdots \\ -\frac{p-1}{2} \equiv \frac{p+1}{2}(\mathrm{mod}\, p) \end{array}\right\} \Rightarrow \tfrac{p-1}{2}! \equiv (p-1)\,(p-2) \cdots \tfrac{p+1}{2}(\mathrm{mod}\, p). \tag{5.82}$$

Συνδυάζοντας τις (5.81) και (5.82) λαμβάνουμε

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

Από το θεώρημα 5.7.1 τού Wilson, $(p-1)! \equiv -1(\mathrm{mod}\, p)$, οπότε

$$\left(\tfrac{p-1}{2}!\right)^2 \equiv -1\,(\mathrm{mod}\ p)\,,$$

λόγω τής μεταβατικότητας τής σχέσεως ισοτιμίας κατά μόδιο p.

Εν συνεχεία, ας υποθέσουμε ότι $p \equiv 3(\mathrm{mod}\ 4)$. Τότε θα υπάρχει ένας ακέραιος k, ούτως ώστε να ισχύει η ισότητα: $p = 4k + 3$. Επομένως,

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

οπότε $-\left(\frac{p-1}{2}!\right)^2 \equiv 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \frac{p+1}{2} \cdots (p-1) \equiv (p-1)! \equiv -1(\mathrm{mod}\ p)$, εκ νέου κατόπιν εφαρμογής τού θεωρήματος τού Wilson. □

5.7.3 Θεώρημα. *Έστω p ένας πρώτος αριθμός. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Ο p είναι ανάγωγο στοιχείο τού δακτυλίου $\mathbb{Z}[i]$ των ακεραίων τού Gauss.*

(ii) $p \equiv 3(\mathrm{mod}\ 4)$.

(iii) *Ο p δεν γράφεται υπό τη μορφή $p = a^2 + b^2$, όπου $a, b \in \mathbb{Z}$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii): Ας υποθέσουμε ότι $p \not\equiv 3(\mathrm{mod}\ 4)$. Εάν $p = 2$, τότε έχουμε $2 = (1+i)\,(1-i)$ με $1 \pm i \notin \mathbb{Z}[i]^\times$, οπότε ο p δεν είναι ανάγωγο στοιχείο. Εάν, από την άλλη μεριά, ο $p \neq 2$, τότε $p \equiv 1(\mathrm{mod}\ 4)$ και, σύμφωνα με το πόρισμα 5.7.2, ο αριθμός $x := \frac{p-1}{2}!$ πληροί την ισοτιμία

$$x^2 \equiv -1(\mathrm{mod}\ p) \Rightarrow p \mid x^2 + 1 \Rightarrow p \mid (x+i)\,(x-i)$$

(με την τελευταία σχέση διαιρετότητας ισχύουσα εντός τού $\mathbb{Z}[i]$). Εάν υποθέταμε ότι $p \mid x + \varepsilon$, για κάποιο $\varepsilon \in \{\pm i\}$, θα υπήρχαν $u, v \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα

$$x + \varepsilon = p\,(u + iv) \Rightarrow x = pu, \;\; pv \in \{\pm 1\},$$

απ' όπου θα καταλήγαμε σε κάτι το οποίο είναι άτοπο. Άρα $p \nmid x + \varepsilon$ για οιοδήποτε $\varepsilon \in \{\pm i\}$, πράγμα που σημαίνει ότι ο p δεν είναι πρώτο στοιχείο τού $\mathbb{Z}[i]$, και, κατ' επέκταση, ούτε ανάγωγο (διότι ο $\mathbb{Z}[i]$ είναι Π.Κ.Ι., βλ. 4.2.11 και 5.3.4 (iv)).

(ii)⇒(iii): Έστω ότι ο p γράφεται υπό τη μορφή $p = a^2 + b^2$, όπου $a, b \in \mathbb{Z}$. Επειδή το τετράγωνο κάθε ακεραίου είναι ισότιμο είτε με 0 είτε με 1 κατά μόδιο 4 και επειδή $4 \nmid p$, έχουμε είτε $p \equiv 1(\mathrm{mod}\ 4)$ είτε[35] $p \equiv 2(\mathrm{mod}\ 4)$.

(iii)⇒(i): Έστω ότι το p δεν είναι ανάγωγο στοιχείο τού δακτυλίου $\mathbb{Z}[i]$. Τότε υπάρχουν ακέραιοι αριθμοί a, b, c, d,τέτοιοι ώστε να ισχύει η ισότητα

$$p = (a+bi)\,(c+di),$$

με κανέναν εκ των $a + bi$ και $c + di$ αντιστρέψιμο (οπότε $|ab| \geq 1$ και, αντιστοίχως, $|cd| \geq 1$). Κατά συνέπειαν,

$$\left.\begin{array}{l} p = (a+bi)\,(c+di) \\ p = (a-bi)\,(c-di) \end{array}\right\} \Rightarrow p^2 = \left(a^2+b^2\right)\left(c^2+d^2\right).$$

[35] Προφανώς, για p πρώτο, έχουμε $p \equiv 2(\mathrm{mod}\ 4) \iff p = 2$.

Επειδή $a^2+b^2 \geq 2$ και $c^2+d^2 \geq 2$, και ο p είναι πρώτος αριθμός, έχουμε

$$p = a^2+b^2 \ \left(= c^2+d^2\right),$$

δηλαδή ο p γράφεται ως άθροισμα τετραγώνων δύο ακεραίων αριθμών. □

5.7.4 Θεώρημα. *Τα ανάγωγα στοιχεία τού δακτυλίου $\mathbb{Z}[i]$ των γκαουσιανών ακεραίων είναι τής μορφής*:

(i) $\pm p, \pm ip$, *όπου p πρώτος αριθμός με* $p \equiv 3 (\mathrm{mod}\ 4)$, *και*

(ii) *στοιχεία $z = a+bi \in \mathbb{Z}[i]$ με $\mathbf{N}(z) = a^2+b^2$ έναν πρώτο αριθμό.*

ΑΠΟΔΕΙΞΗ. Το ότι τα στοιχεία τού $\mathbb{Z}[i]$ που είναι τής μορφής (i) είναι ανάγωγα έπεται άμεσα από το θεώρημα 5.7.3 και το ότι $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Το ότι τα στοιχεία τού $\mathbb{Z}[i]$ που είναι τής μορφής (ii) είναι ανάγωγα έπεται από την πρόταση 5.3.9.

Και αντιστρόφως· εάν το $q = a+bi$ είναι τυχόν ανάγωγο στοιχείο τού $\mathbb{Z}[i]$, όπου $a, b \in \mathbb{Z}$, τότε, στην περίπτωση κατά την οποία $b = 0$, έχουμε $q \in \mathbb{Z}$, οπότε υπάρχει πρώτος αριθμός p με

$$q = \pm p \Longrightarrow p \text{ ανάγωγο στοιχείο} \underset{5.7.3}{\Longrightarrow} p \equiv 3 (\mathrm{mod}\ 4)$$

και, κατ' αναλογίαν, στην περίπτωση κατά την οποία $a = 0$, έχουμε $q = \pm ip$ με $p \equiv 3 (\mathrm{mod}\ 4)$. Εξάλλου, όταν έχουμε $a \neq 0$ και $b \neq 0$, η αριθμητική στάθμη $\mathbf{N}(q)$ τού q οφείλει να είναι ένας *πρώτος αριθμός*. Πράγματι· εξαιτίας τού ότι η απεικόνιση $\mathbb{Z}[i] \ni z \longmapsto \overline{z} \in \mathbb{Z}[i]$ είναι ένας ισομορφισμός, *και* το $\overline{q} = a-ib$ είναι ανάγωγο στοιχείο τού $\mathbb{Z}[i]$. Εάν λοιπόν υποθέταμε ότι ο αριθμός $\mathbf{N}(q) = a^2+b^2$ είναι σύνθετος, θα υπήρχαν ακέραιοι $c, d > 1$, τέτοιοι ώστε να ισχύει η ισότητα

$$a^2+b^2 = (a+bi)(a-bi) = cd.$$

Αυτό θα σήμαινε *είτε* ότι αμφότερα τα c, d είναι ανάγωγα (κάτι το οποίο, συνδυαζόμενο με το γεγονός ότι ο $\mathbb{Z}[i]$ είναι Π.Μ.Π., θα μας οδηγούσε σε άτοπο, αφού θα έπρεπε να ισχύει $q \underset{\text{συν.}}{\sim} c$ ή $q \underset{\text{συν.}}{\sim} d$) *είτε* ότι ένα εξ αυτών δεν είναι ανάγωγο. Αλλά *και* αυτό το ενδεχόμενο αποκλείεται, καθόσον στο αριστερό μέλος τής ανωτέρω ισότητας θα εμφανιζόταν ένα γινόμενο δύο αναγώγων στοιχείων και στο δεξιό της μέλος ένα γινόμενο *τουλάχιστον τριών* αναγώγων στοιχείων. □

5.7.5 Λήμμα. *Έστω p ένας πρώτος αριθμός με $p \equiv 1 (\mathrm{mod}\ 4)$ και έστω ρ ένα πρώτο στοιχείο τού $\mathbb{Z}[i]$, το οποίο διαιρεί τον p (εντός τού $\mathbb{Z}[i]$). Τότε ο συζυγής $\overline{\rho}$ τού ρ είναι ένα πρώτο στοιχείο τού $\mathbb{Z}[i]$, το οποίο δεν είναι συντροφικό τού ρ, και $p = \rho\overline{\rho}$.*

ΑΠΟΔΕΙΞΗ. Εφαρμόζοντας εκ νέου το πόρισμα 5.7.2 για τον $x := \frac{p-1}{2}!$ έχουμε

$$x^2 \equiv -1 (\mathrm{mod}\ p) \Rightarrow p \mid x^2+1 = (x+i)(x-i) \left.\begin{array}{r} \\ \rho \mid p \end{array}\right\} \Rightarrow \rho \mid (x+i)(x-i),$$

οπότε είτε $\rho \mid x+i$ είτε $\rho \mid x-i$. Επειδή $p \nmid x+i$ και $p \nmid x-i$, τα p και ρ δεν είναι συντροφικά. Προφανώς,

$$\left.\begin{array}{r} \mathbf{N}(\rho) \neq \mathbf{N}(p) = p^2, \ \ \mathbf{N}(\rho) \neq 1 \\ \mathbf{N}(\rho) \mid \mathbf{N}(p) \end{array}\right\} \Rightarrow p = \mathbf{N}(\rho) = \rho\overline{\rho}.$$

Και επειδή $\mathbf{N}(\rho) = \mathbf{N}(\overline{\rho}) = p$, *και* το $\overline{\rho}$ είναι ένα πρώτο στοιχείο τού $\mathbb{Z}[i]$. Υπολείπεται τα δείξουμε ότι τα ρ και $\overline{\rho}$ δεν είναι συντροφικά. Ας υποθέσουμε ότι $\rho \underset{\text{συν.}}{\sim} \overline{\rho}$. Γράφοντας το ρ ως $\rho = a+bi$, όπου $a, b \in \mathbb{Z}$, εξετάζουμε τις τέσσερεις περιπτώσεις:

Περίπτωση πρώτη. Εάν $\rho = \overline{\rho}$, τότε $\rho = a$ και $p = a^2$.

Περίπτωση δεύτερη. Εάν $\rho = -\overline{\rho}$, τότε $\rho = ib$ και $p = b^2$.

Περίπτωση τρίτη. Εάν $\rho = i\overline{\rho}$, τότε $a = -b$ και $p = 2a^2$.

Περίπτωση τέταρτη. Εάν $\rho = -i\overline{\rho}$, τότε $a = b$ και $p = 2a^2$.

Και στις τέσσερεις περιπτώσεις καταλήγουμε σε *άτοπο*, αφού ο p είναι πρώτος αριθμός με $p \equiv 1 (\mathrm{mod}\ 4)$. Ως εκ τούτου, τα ρ και $\overline{\rho}$ δεν είναι συντροφικά. □

5.7.6 Πόρισμα. *Εάν $z = a+bi \in \mathbb{Z}[i]$ με το $\mathbf{N}(z) = a^2+b^2$ ίσο με έναν πρώτο αριθμό $p > 2$, τότε $p = \rho_p\overline{\rho_p}$, για κάποια συζυγή, πρώτα (και, κατ' επέκταση, ανάγωγα) στοιχεία ρ_p και $\overline{\rho_p}$ τού $\mathbb{Z}[i]$, τα οποία δεν συντροφικά. Επιπροσθέτως,*

$$\text{είτε } \left(z \underset{\text{συν.}}{\sim} \rho_p \text{ και } \overline{z} \underset{\text{συν.}}{\sim} \overline{\rho_p}\right) \text{ είτε } \left(z \underset{\text{συν.}}{\sim} \overline{\rho_p} \text{ και } \overline{z} \underset{\text{συν.}}{\sim} \rho_p\right).$$

ΑΠΟΔΕΙΞΗ. Επειδή $p > 2$ και $p = a^2 + b^2$, το θεώρημα 5.7.3 μας πληροφορεί ότι $p \equiv 1 (\mathrm{mod}\ 4)$. Επειδή ο ίδιος ο p *δεν* είναι ανάγωγο στοιχείο τού $\mathbb{Z}[i]$ (βλ. 5.7.3) το λήμμα 5.7.5 μας υποδεικνύει το πώς μπορούμε να τον παραγοντοποιήσουμε υπό τη μορφή $p = \rho_p\overline{\rho_p}$ μέσω κάποιων συζυγών, πρώτων (και, κατ' επέκταση, αναγώγων) στοιχείων ρ_p και $\overline{\rho_p}$ τού $\mathbb{Z}[i]$, τα οποία δεν συντροφικά. (Βεβαίως, τα ρ_p και $\overline{\rho_p}$ είναι μονοσημάντως ορισμένα, με μόνη εξαίρεση την αντικατάσταση τουλάχιστον ενός εξ αυτών με κάποιον κατάλληλο σύντροφό του.) Επιπροσθέτως, λόγω τής παραστάσεως τού p ως γινομένου αναγώγων στοιχείων κατά δύο τρόπους:

$$p = (a+bi)(a-bi) = \rho_p\overline{\rho_p},$$

και ο τελευταίος ισχυρισμός είναι αληθής (καθότι ο $\mathbb{Z}[i]$ είναι Π.Μ.Π.). □

5.7.7 Λήμμα. *Το γινόμενο δύο ακεραίων, καθένας των οποίων ισούται με το άθροισμα των τετραγώνων δύο ακεραίων, είναι αφ' εαυτού άθροισμα τετραγώνων δύο ακεραίων αριθμών.*

ΑΠΟΔΕΙΞΗ. Επειδή για οιουσδήποτε $a, b, c, d \in \mathbb{Z}$ ισχύει η ισότητα

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = (ac-bd)^2 + (ad+bc)^2,$$

ο ισχυρισμός είναι αληθής. □

5.7.8 Θεώρημα. (Πότε είναι ένας $n \in \mathbb{N}$ άθροισμα δύο τετραγώνων;) *Για έναν $n \in \mathbb{N}$ οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Ο n ισούται με το άθροισμα των τετραγώνων δύο ακεραίων αριθμών.*

(ii) *Στην παράσταση τού n ως γινομένου πρώτων αριθμών, κάθε πρώτος παράγοντάς του που είναι $\equiv 3(\mathrm{mod}\ 4)$ εμφανίζεται υψωμένος σε κάποια άρτια δύναμη.*

ΑΠΟΔΕΙΞΗ[36]. Η παράσταση οιουδήποτε $n \in \mathbb{N}$ ως γινομένου πρώτων αριθμών μπορεί να γραφεί ως ακολούθως:

$$n = 2^{\lambda} \left(\prod_{p \text{ πρώτος, } p \equiv 1(\mathrm{mod}\ 4)} p^{\beta_p} \right) \left(\prod_{q \text{ πρώτος, } q \equiv 3(\mathrm{mod}\ 4)} q^{\gamma_q} \right), \tag{5.83}$$

όπου[37] $\lambda, \beta_p = \boldsymbol{\nu}_p(n), \gamma_q = \boldsymbol{\nu}_q(n) \in \mathbb{N}_0$. Αρκεί λοιπόν να δείξουμε ότι

$$[\exists x, y \in \mathbb{Z} : n = x^2 + y^2] \Leftrightarrow \left[\gamma_q \equiv 0(\mathrm{mod}\ 2), \forall \text{ πρώτον } q \text{ με } q \equiv 3(\mathrm{mod}\ 4)\right].$$

(i)⇒(ii): Έστω ότι $\exists x, y \in \mathbb{Z} : n = x^2 + y^2 = (x + yi)(x - yi)$. Λόγω τού θεωρήματος 5.7.4, τού πορίσματος 5.7.6 και τού γεγονότος ότι ο $\mathbb{Z}[i]$ είναι Π.Μ.Π., η παράσταση τού $x + yi$ ως γινομένου πρώτων στοιχείων γράφεται ως ακολούθως:

$$x + yi = \varepsilon\ (1+i)^{\lambda} \left(\prod_{p \text{ πρώτος, } p \equiv 1(\mathrm{mod}\ 4)} \rho_p^{\mu_p} \overline{\rho_p}^{\mu'_p} \right) \left(\prod_{q \text{ πρώτος, } q \equiv 3(\mathrm{mod}\ 4)} q^{\eta_q} \right),$$

όπου $\varepsilon \in \{\pm 1, \pm i\}$ και $\mu_p, \mu'_p, \eta_q \in \mathbb{N}_0$. Σχηματίζοντας τον συζυγή του

$$x - yi = \overline{\varepsilon}\ (1-i)^{\lambda} \left(\prod_{p \text{ πρώτος, } p \equiv 1(\mathrm{mod}\ 4)} \overline{\rho_p}^{\mu_p} \rho_p^{\mu'_p} \right) \left(\prod_{q \text{ πρώτος, } q \equiv 3(\mathrm{mod}\ 4)} \overline{q}^{\eta_q} \right)$$

και πολλαπλασιάζοντας τις δύο αυτές ισότητες κατά μέλη λαμβάνουμε

$$n = \varepsilon^2\ 2^{\lambda} \left(\prod_{p \text{ πρώτος, } p \equiv 1(\mathrm{mod}\ 4)} p^{\mu_p + \mu'_p} \right) \left(\prod_{q \text{ πρώτος, } q \equiv 3(\mathrm{mod}\ 4)} \overline{q}^{2\eta_q} \right),\ \varepsilon^2 \in \{\pm 1\},$$

[36] Το θεώρημα 5.7.8 διατυπώθηκε ως εικασία το 1641 από τον Fermat (1601-1665). Η πρώτη του απόδειξη ανακαλύφθηκε από τον L. Euler (1707-1783) και βασίζεται στη *μέθοδο τής επ' άπειρον καταβάσεως*. (Αυτός την προανήγγειλε σε δύο επιστολές του απευθυνθείσες στον Ch. Goldbach, την 6η Μαΐου 1747 και την 12η Απριλίου 1749, αντιστοίχως, και τη δημοσίευσε με κάθε λεπτομέρεια αργότερα, σε δύο άρθρα του μεταξύ των ετών 1752 και 1755.) Ο J.-L. Lagrange (1736-1813) έδωσε το 1775 μια άλλη απόδειξη προκύπτουσα από τη μελέτη του περί των τετραγωνικών μορφών. Αυτή η απόδειξη απλοποιήθηκε από τον C.F. Gauss (1777-1855) στο εδάφιο 182 των *Disquisitiones Arithmeticae* (1801). Τέλος, ο R. Dedekind (1831-1916) προσέθεσε δύο ακόμη αποδείξεις (1877 και 1894) χρησιμοποιώντας περιτέχνως τις ιδιότητες των γκαουσιανών ακεραίων. Η απόδειξη που παρατίθεται εδώ αποτελεί ελαφρά παραλλαγή τής δεύτερης εξ αυτών.

[37] Όταν $n = 1$, τότε $\lambda = \beta_p = \gamma_q = 0$.

απ' όπου έπεται ότι το ε^2 ισούται κατ' ανάγκην με το 1 και ότι $\gamma_q = 2\eta_q \equiv 0 (\mathrm{mod}\ 2)$ για κάθε πρώτο q με $q \equiv 3 (\mathrm{mod}\ 4)$.

(ii)⇒(i): Έστω ότι ο εκθέτης γ_q είναι άρτιος για κάθε πρώτο αριθμό q τής παραστάσεως (5.83) τού n όταν $q \equiv 3 (\mathrm{mod}\ 4)$. Τότε επί τη βάσει τού θεωρήματος 5.7.3 έχουμε τη δυνατότητα να γράψουμε κάθε πρώτο αριθμό p τής παραστάσεως (5.83) τού n, όπου $p \equiv 1 (\mathrm{mod}\ 4)$, υπό τη μορφή $p = x_p^2 + y_p^2$, για καταλλήλους $x_p, y_p \in \mathbb{Z}$. Μια σύντομη απόδειξη για το ότι ο n ισούται με το άθροισμα των τετραγώνων δύο ακεραίων αριθμών μάς αποκαλύπτεται παρατηρώντας ότι $n = \mathbf{N}(z) = z\overline{z}$, όπου

$$z := (1+i)^{\lambda} \left(\prod_{p \text{ πρώτος},\ p \equiv 1 (\mathrm{mod}\ 4)} (x_p + y_p i)^{\beta_p} \right) \left(\prod_{q \text{ πρώτος},\ q \equiv 3 (\mathrm{mod}\ 4)} q^{\frac{\gamma_q}{2}} \right).$$

Εκφράζοντας τον z υπό τη μορφή $z = x + yi$, για καταλλήλους $x, y \in \mathbb{Z}$, λαμβάνουμε αυτομάτως: $n = x^2 + y^2$. Μια άλλη απόδειξη έχει ως εξής: Γράφουμε τον n ως

$$n = 2^{\lambda} \left(\prod_{p \text{ πρώτος},\ p \equiv 1 (\mathrm{mod}\ 4)} (x_p^2 + y_p^2) \right) \left(\prod_{q \text{ πρώτος},\ q \equiv 3 (\mathrm{mod}\ 4)} \left(q^{\frac{\gamma_q}{2}} \right)^2 \right),$$

παρατηρούμε ότι $2^{\lambda} = \left(1^2 + 1^2\right)^{\lambda}$ και $(q^{\frac{\gamma_q}{2}})^2 = 0^2 + (q^{\frac{\gamma_q}{2}})^2$, και κατόπιν εφαρμόζουμε το λήμμα 5.7.7. □

5.7.9 Παρατήρηση. Ένας φυσικός αριθμός ενδέχεται να γράφεται ως άθροισμα δύο τετραγώνων κατά διαφορετικούς τρόπους. Επί παραδείγματι,

$$325 = 5^2 \cdot 13 = 1^2 + 18^2 = 6^2 + 17^2 = 10^2 + 15^2.$$

► **Πρώτοι τής μορφής** $p = x^2 + ny^2$ ($x, y \in \mathbb{Z}$, $n \in \mathbb{Z} \setminus \{0\}$). Αυτοί οι πρώτοι αριθμοί (που παριστώνται ως ειδικοί ακέραιοι γραμμικοί συνδυασμοί δύο τετραγώνων) ή, γενικότερα, οι πρώτοι αριθμοί που είναι παραστάσιμοι μέσω μιας δυαδικής ακεραίας τετραγωνικής μορφής[38], έχουν μακραίωνη ιστορία, έχουν απασχολήσει σωρεία επιφανών μαθηματικών και καταλαμβάνουν αρκετά κεφάλαια εντός τού πλαισίου τής Αλγεβρικής Θεωρίας Αριθμών[39]. Εδώ θα μελετήσουμε μόνον ορισμένους εξ αυτών σε *ειδικές περιπτώσεις*: Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων και έστω p ένας *περιττός πρώτος αριθμός που δεν διαιρεί τον* m. Όταν $m \not\equiv 1 (\mathrm{mod}\ 4)$, τότε σύμφωνα με το λήμμα 5.7.10 ισχύει η συνεπαγωγή[40]

$$\boxed{\left[\exists x, y \in \mathbb{Z} : p = \left|x^2 - my^2\right|\right] \Rightarrow \left(\tfrac{m}{p}\right) = 1,} \qquad (5.84)$$

[38] Αυτό σημαίνει ότι $p = ax^2 + bxy + cy^2$, όπου $x, y \in \mathbb{Z}$ και οι a, b, c είναι *παγιωμένοι* ακέραιοι.

[39] Βλ. D.A. Cox: *Primes of the Form* $x^2 + ny^2$, 2nd ed., John Wiley & Sons, Inc., 2013.

[40] Στην περίπτωση όπου ο m είναι *αρνητικός*, οι απόλυτες τιμές στις (5.84) και (5.85) μπορούν να αφαιρεθούν.

ενώ όταν $m \equiv 1 (\mathrm{mod}\ 4)$,

$$\boxed{\left[\exists x, y \in \mathbb{Z} : p = \left|x^2 + xy + \tfrac{y^2}{4}(1-m)\right|\right] \Rightarrow \left(\tfrac{m}{p}\right) = 1,} \tag{5.85}$$

όπου $\left(\frac{m}{p}\right)$ είναι το *σύμβολο τού Legendre*. (Βλ. ορισμό 5.7.14.) Μάλιστα, στην περίπτωση κατά την οποία ο δακτύλιος $\mathfrak{O}_m$ είναι Π.Μ.Π., από την ισοδυναμία (i)⇔(iv) στο θεώρημα 5.7.11 (που γενικεύει το θεώρημα 5.7.3) έπεται ότι οι (5.84) και (5.85) ισχύουν ως *αμφίπλευρες* συνεπαγωγές

$$\boxed{\left[\exists x, y \in \mathbb{Z} : p = \left|x^2 - my^2\right|\right] \Leftrightarrow \left(\tfrac{m}{p}\right) = 1,} \tag{5.86}$$

όταν $m \not\equiv 1 (\mathrm{mod}\ 4)$ και

$$\boxed{\left[\exists x, y \in \mathbb{Z} : p = \left|x^2 + xy + \tfrac{y^2}{4}(1-m)\right|\right] \Leftrightarrow \left(\tfrac{m}{p}\right) = 1,} \tag{5.87}$$

όταν $m \equiv 1 (\mathrm{mod}\ 4)$. Η ισότητα $\left(\frac{m}{p}\right) = 1$ ισχύει για *απειροπληθείς* περιττούς πρώτους αριθμούς p. Δειγματοληπτικώς, στο θεώρημα 5.7.31 καταγράφουμε, μεταξύ άλλων, το ποιοι ακριβώς είναι αυτοί οι πρώτοι αριθμοί στην περίπτωση κατά την οποία $|m| \leq 7$.

5.7.10 Λήμμα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν υπάρχει στοιχείο $z \in \mathfrak{O}_m$ με $|\mathbf{N}(z)| = p$, όπου p ένας περιττός πρώτος αριθμός, τότε $k^2 \equiv m (\mathrm{mod}\, p)$ για κάποιον $k \in \mathbb{Z}$.*

ΑΠΟΔΕΙΞΗ. Εάν υπάρχει $z \in \mathfrak{O}_m$ με $|\mathbf{N}(z)| = p$, όπου

$$z = \begin{cases} x + y\sqrt{m}, & \text{όταν } p \not\equiv 1 (\mathrm{mod}\ 4), \\ \\ x + y\frac{1+\sqrt{m}}{2}, & \text{όταν } p \equiv 1 (\mathrm{mod}\ 4), \end{cases}$$

για κάποιους $x, y \in \mathbb{Z}$, τότε $p \nmid y$. Πράγματι· εάν ίσχυε $p \mid y$, τότε θα είχαμε

$$p \mid \pm p = \mathbf{N}(z) = z\overline{z} = \begin{cases} x^2 - my^2, & \text{όταν } p \not\equiv 1 (\mathrm{mod}\ 4), \\ \\ x^2 + xy + \frac{y^2}{4}(1-m), & \text{όταν } p \equiv 1 (\mathrm{mod}\ 4), \end{cases}$$

απ' όπου θα έπετο ότι $p \mid x^2 \underset{p\ \text{πρώτος}}{\Longrightarrow} p \mid x$ και, κατ' επέκταση, ότι

$$\left.\begin{aligned} p \mid x \Rightarrow p^2 \mid x^2 \\ p \mid y \Rightarrow p^2 \mid y^2 \\ p^2 \mid xy \end{aligned}\right\} \Rightarrow p^2 \mid \mathbf{N}(z),$$

κάτι που θα αντέκειτο στην υπόθεση ότι $\mathbf{N}(z) = \pm p$. Το ότι $p \nmid y$ συνεπάγεται την ύπαρξη ενός (και μόνον) $\eta \in \mathbb{Z}$ με $y\eta \equiv 1 (\mathrm{mod}\, p)$. (Βλ. πόρισμα 3.4.2.) Άρα $y\eta - 1 = pl$ για κάποιον $l \in \mathbb{Z}$.

Περίπτωση πρώτη. Εάν $p \not\equiv 1 (\mathrm{mod}\, 4)$, τότε θέτοντας $k := x\eta$ λαμβάνουμε

$$\begin{aligned} &\pm p\eta^2 = (x^2 - my^2)\eta^2 = k^2 - m\,(pl+1)^2 \\ &\Rightarrow k^2 = m + p(mpl^2 + 2ml \pm \eta^2) \Rightarrow k^2 \equiv m (\mathrm{mod}\, p). \end{aligned}$$

Περίπτωση δεύτερη. Εάν $p \equiv 1 (\mathrm{mod}\, 4)$, τότε θέτοντας $k := (2x+y)\,\eta$ λαμβάνουμε

$$\begin{aligned} &\pm 4p = 4x^2 + 4xy + y^2(1-m) = (2x+y)^2 - my^2 \\ &\Rightarrow \pm 4p\eta^2 = k^2 - m\,(y\eta)^2 = k^2 - m\,(pl+1)^2 \\ &\Rightarrow k^2 = m + p(mpl^2 + 2ml \pm 4\eta^2) \Rightarrow k^2 \equiv m (\mathrm{mod}\, p), \end{aligned}$$

οπότε *και* σε αυτήν την περίπτωση ο ισχυρισμός είναι αληθής. □

5.7.11 Θεώρημα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν ο δακτύλιος $\mathfrak{O}_m$ των ακεραίων τού $\mathbb{Q}(\sqrt{m})$ είναι Π.Μ.Π., τότε για κάθε περιττό πρώτον αριθμό p οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\exists k \in \mathbb{Z} : k^2 \equiv m (\mathrm{mod}\, p)$.

(ii) *Ο p δεν είναι πρώτο στοιχείο τής $\mathfrak{O}_m$.*

(iii) *Ο p ισούται με το γινόμενο δύο πρώτων στοιχείων τής $\mathfrak{O}_m$, καθένα των οποίων έχει αριθμητική στάθμη $\pm p$.*

(iv) $\exists z \in \mathfrak{O}_m : |\mathbf{N}(z)| = p$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εξ υποθέσεως, υπάρχει $k \in \mathbb{Z}$ με

$$p \mid k^2 - m = \left(k + \sqrt{m}\right)\left(k - \sqrt{m}\right).$$

Εντός τής $\mathfrak{O}_m$, $p \nmid k \pm \sqrt{m}$, διότι $\frac{k}{p} \pm \frac{k}{p}\sqrt{m} \in \mathbb{Q}(\sqrt{m}) \setminus \mathfrak{O}_m$. Επομένως ο p δεν είναι πρώτο στοιχείο τής $\mathfrak{O}_m$.

(ii)⇒(iii) Επειδή $\mathbf{N}(p) = p^2 \neq \pm 1 \Rightarrow p \notin \mathfrak{O}_m^\times$ και η $\mathfrak{O}_m$ είναι περιοχή με παραγοντοποίηση, θα υπάρχει κάποιο ανάγωγο στοιχείο $u \in \mathfrak{O}_m \setminus \left(\mathfrak{O}_m^\times \cup \{0\}\right)$, τέτοιο ώστε να ισχύει $u \mid p$ (εντός τής $\mathfrak{O}_m$), οπότε $p = uw$ για κάποιο $w \in \mathfrak{O}_m$. Το w δεν είναι αντιστρέψιμο στοιχείο, διότι εξ υποθέσεως το p δεν είναι πρώτο (και, ως εκ τούτου, δεν είναι ανάγωγο, αφού η $\mathfrak{O}_m$ είναι Π.Μ.Π., βλ. 5.6.3). Προφανώς,

$$\left.\begin{aligned} p^2 = \mathbf{N}(p) &= \mathbf{N}(u)\mathbf{N}(w) \\ u \notin \mathfrak{O}_m^\times &\Rightarrow \mathbf{N}(u) \neq \pm 1 \\ w \notin \mathfrak{O}_m^\times &\Rightarrow \mathbf{N}(w) \neq \pm 1 \end{aligned}\right\} \Rightarrow \mathbf{N}(u) \in \{\pm p\} \text{ και } \mathbf{N}(w) \in \{\pm p\},$$

οπότε αμφότερα τα u, w είναι ανάγωγα και, ως εκ τούτου, πρώτα στοιχεία τής Π.Μ.Π. $\mathfrak{O}_m$. (Βλ. 5.3.9, 5.5.3 (ii) και 5.6.3.)

(iii)⇒(iv) Τούτο είναι προφανές.

(iv)⇒(i) Βλ. λήμμα 5.7.10. □

5.7.12 Ορισμός. Έστω $l \in \mathbb{N}$ και έστω $a \in \mathbb{Z}$ με μκδ$(a, l) = 1$. Εάν η ισοτιμία

$$\boxed{x^2 \equiv a (\mathrm{mod}\, l)} \tag{5.88}$$

διαθέτει κάποια (ακεραία) λύση, τότε λέμε ότι ο a είναι ένα[41] **τετραγωνικό ισοϋπόλοιπο** κατά μόδιο l. Εάν η (5.88) δεν διαθέτει καμία λύση, τότε λέμε ότι ο a είναι ένα **τετραγωνικό ανισοϋπόλοιπο** κατά μόδιο l.

5.7.13 Σημείωση. Στην ειδική περίπτωση κατά την οποία $l = p$, όπου p ένας περιττός πρώτος αριθμός, εάν υποτεθεί ότι x_0 είναι μια λύση τής

$$\boxed{x^2 \equiv a (\mathrm{mod}\, p),} \tag{5.89}$$

τότε (επειδή $p \nmid a$) *και* ο $-x_0$ αποτελεί λύση αυτής (και μάλιστα, διαφορετική τής $x_0 \ (\mathrm{mod}\, m)$), και οι $\pm x_0$ είναι *οι μόνες λύσεις* τής (5.89) κατά μόδιο p.

5.7.14 Ορισμός. Έστω p ένας περιττός πρώτος αριθμός και έστω $a \in \mathbb{Z}$ με $p \nmid a$. Το **σύμβολο** $\left(\frac{a}{p}\right)$ **τού Legendre** ορίζεται ως εξής[42]:

$$\boxed{\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{όταν ο } a \text{ είναι τετραγωνικό ισοϋπόλοιπο } (\mathrm{mod}\, p), \\ -1, & \text{όταν ο } a \text{ είναι τετραγωνικό ανισοϋπόλοιπο } (\mathrm{mod}\, p). \end{cases}}$$

5.7.15 Θεώρημα. (Κριτήριο τού Euler, 1736.) *Εάν p είναι ένας περιττός πρώτος αριθμός και $a \in \mathbb{Z}$ με $p \nmid a$, τότε ισχύει η ακόλουθη ισοτιμία*:

$$\boxed{\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} (\mathrm{mod}\, p)\,.} \tag{5.90}$$

ΑΠΟΔΕΙΞΗ[43]. *Περίπτωση πρώτη.* Εάν $\left(\frac{a}{p}\right) = 1$, τότε εξ ορισμού υπάρχει κάποια λύση x_0 τής (5.89). Από το θεώρημα τού Euler περί ισοτιμιών (βλ. εδ. 3.4.3) λαμβάνουμε

$$\left.\begin{aligned} x_0^2 &\equiv a (\mathrm{mod}\, p) \\ x_0^{\phi(p)} = x_0^{p-1} = (x_0^2)^{\frac{p-1}{2}} &\equiv 1 (\mathrm{mod}\, p) \end{aligned}\right\} \Rightarrow a^{\frac{1}{2}(p-1)} \equiv 1 (\mathrm{mod}\, p),$$

[41] Εάν $a \equiv b (\mathrm{mod}\, l)$, για κάποιον $b \in \mathbb{Z}$, τότε είναι προφανές ότι ο a είναι τετραγωνικό ισοϋπόλοιπο κατά μόδιο l εάν και μόνον εάν συμβαίνει το ίδιο και για τον b.

[42] Ορισμένοι συγγραφείς επεκτείνουν αυτόν τον ορισμό ακόμη και όταν $p \mid a$, θέτοντας, εν τοιαύτη περιπτώσει, $\left(\frac{a}{p}\right) := 0$.

[43] Αυτή η απόδειξη οφείλεται στον Peter Gustav Dirichlet (1805-1859).

οπότε η (5.90) είναι αληθής.

Περίπτωση δεύτερη. Υποθέτουμε ότι $\left(\frac{a}{p}\right) = -1$. Εξ ορισμού, δεν υπάρχει καμία λύση τής (5.89). Έστω $c \in \{1, ..., p-1\}$. Ως γνωστόν, η γραμμική ισοτιμία $cx \equiv a (\mathrm{mod}\, p)$ διαθέτει μία και μόνον λύση c' κατά μόδιο p. (Βλ. πόρισμα 3.4.2.) Δίχως βλάβη τής γενικότητας (ήτοι μέχρις αναγωγής $\mathrm{mod}\, p$) μπορούμε να υποθέσουμε ότι $c' \in \{1, ..., p-1\}$. Προφανώς, $c \neq c'$ (διότι αλλιώς ο φυσικός αριθμός c θα αποτελούσε μια λύση τής (5.89)). Κατά συνέπειαν, τα στοιχεία τού συνόλου $\{1, ..., p-1\}$ μπορούν να διαιρεθούν σε διαφορετικά[44] ζεύγη c, c' με $cc' \equiv a (\mathrm{mod}\, p)$. Ας συμβολίσουμε αυτά τα ζεύγη ως $(c_1, c_1'), (c_2, c_2'), \ldots, (c_{\frac{p-1}{2}}, c_{\frac{p-1}{2}}')$. Προφανώς,

$$\left.\begin{array}{c} c_1 c_1' \equiv a (\mathrm{mod}\, p) \\ c_2 c_2' \equiv a (\mathrm{mod}\, p) \\ \vdots \\ c_{\frac{p-1}{2}} c_{\frac{p-1}{2}}' \equiv a (\mathrm{mod}\, p) \end{array}\right\} \Rightarrow \prod_{j=1}^{\frac{p-1}{2}} c_j c_j' = \prod_{j=1}^{p-1} j = (p-1)! \equiv a^{\frac{1}{2}(p-1)} (\mathrm{mod}\, p).$$

Από το θεώρημα 5.7.1 τού Wilson, $(p-1)! \equiv -1 (\mathrm{mod}\, p)$, οπότε η (5.90) είναι αληθής *και* σε αυτήν την περίπτωση. □

5.7.16 Πόρισμα. *Εάν p είναι ένας περιττός πρώτος αριθμός και $a \in \mathbb{Z}$ με $p \nmid a$, τότε*

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow a^{\frac{1}{2}(p-1)} \equiv 1 (\mathrm{mod}\, p)$$
$$\text{και}$$
$$\left(\frac{a}{p}\right) = -1 \Leftrightarrow a^{\frac{1}{2}(p-1)} \equiv -1 (\mathrm{mod}\, p).$$

ΑΠΟΔΕΙΞΗ. Οι συνεπαγωγές "⇒" έχουν αποδειχθεί. Εάν ίσχυε $a^{\frac{1}{2}(p-1)} \equiv 1 (\mathrm{mod}\, p)$ και $\left(\frac{a}{p}\right) = -1$, τότε θα είχαμε

$$\left.\begin{array}{c} a^{\frac{1}{2}(p-1)} \equiv 1 (\mathrm{mod}\, p) \\ a^{\frac{1}{2}(p-1)} \equiv -1 (\mathrm{mod}\, p) \end{array}\right\} \Rightarrow 1 \equiv -1 (\mathrm{mod}\, p) \Rightarrow p \mid 2 \Rightarrow p = 2.$$

Άτοπο! Παρομοίως, εάν ίσχυε $a^{\frac{1}{2}(p-1)} \equiv -1 (\mathrm{mod}\, p)$ και $\left(\frac{a}{p}\right) = 1$, τότε θα καταλήγαμε (με την ίδια συλλογιστική) εκ νέου σε άτοπο. □

5.7.17 Πρόταση. *Έστω p ένας περιττός πρώτος αριθμός. Για $a, b \in \mathbb{Z}$ με $p \nmid a$ και $p \nmid b$ ισχύουν τα εξής:*

(i) $a \equiv b (\mathrm{mod}\, p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $\left(\frac{a^2}{p}\right) = 1$.

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

[44] Εάν b είναι ένα στοιχείο τού $\{1, ..., p-1\}$ διάφορο των c, c', τότε το στοιχείο που θα αντιστοιχεί σε αυτό θα είναι κάποιο $b' \notin \{c, c'\}$. Πράγματι· εάν ίσχυε $b' = c$, τότε θα είχαμε $bc' \equiv a \equiv cc' (\mathrm{mod}\, p)$, και εάν ίσχυε $b' = c'$, τότε θα είχαμε $cb' \equiv a \equiv cc' (\mathrm{mod}\, p)$, καταλήγοντας (σε αμφότερες τις περιπτώσεις) σε άτοπο (διότι $b \notin \{c, c'\}$).

(iv) $\left(\frac{1}{p}\right) = 1$ *και*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)} = \begin{cases} 1, & \text{όταν } p \equiv 1 (\mathrm{mod}\, 4), \\ \\ -1, & \text{όταν } p \equiv 3 (\mathrm{mod}\, 4). \end{cases} \tag{5.91}$$

ΑΠΟΔΕΙΞΗ. (i) Εάν $a \equiv b (\mathrm{mod}\, p)$, τότε είναι πρόδηλο ότι η $x^2 \equiv a (\mathrm{mod}\, p)$ διαθέτει κάποια λύση εάν και μόνο εάν συμβαίνει το ίδιο και για την $x^2 \equiv b (\mathrm{mod}\, p)$.

(ii) Τούτο προκύπτει άμεσα από το (iii), καθότι $\left(\frac{a}{p}\right) \in \{\pm 1\}$.

(iii) Επειδή $[p \nmid a \text{ και } p \nmid b] \Rightarrow p \nmid ab$, το $\left(\frac{ab}{p}\right)$ ορίζεται καλώς και το κριτήριο 5.7.15 τού Euler μάς πληροφορεί ότι

$$\left.\begin{aligned} \left(\tfrac{ab}{p}\right) &\equiv (ab)^{\frac{1}{2}(p-1)} \,(\mathrm{mod}\, p) \\ (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} &\equiv \left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right) (\mathrm{mod}\, p) \end{aligned}\right\} \Rightarrow \left(\tfrac{ab}{p}\right) \equiv \left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right) (\mathrm{mod}\, p)\,.$$

Καθένα εκ των $\left(\frac{ab}{p}\right)$ και $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ ισούται είτε με 1 είτε με -1, οπότε

$$\left.\begin{aligned} p \mid \left(\tfrac{ab}{p}\right) - \left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right) \in \{0, \pm 2\} \\ p \neq 2 \Rightarrow p \nmid \pm 2 \end{aligned}\right\} \Rightarrow \left(\tfrac{ab}{p}\right) = \left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right).$$

(iv) Η πρώτη ισότητα είναι προφανής (λόγω τού (ii) στην περίπτωση όπου $a = 1$). Για την απόδειξη τής (5.91) χρησιμοποιούμε εκ νέου το κριτήριο 5.7.15 τού Euler: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{1}{2}(p-1)} \,(\mathrm{mod}\, p)$. Καθένα εκ των $\left(\frac{-1}{p}\right)$ και $(-1)^{\frac{1}{2}(p-1)}$ ισούται είτε με 1 είτε με -1, οπότε

$$\left.\begin{aligned} p \mid \left(\tfrac{-1}{p}\right) - (-1)^{\frac{1}{2}(p-1)} \in \{0, \pm 2\} \\ p \neq 2 \Rightarrow p \nmid \pm 2 \end{aligned}\right\} \Rightarrow \left(\tfrac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}.$$

Σημειωτέον ότι

$$\tfrac{1}{2}(p-1) = \begin{cases} 2k, & \text{όταν } \exists k \in \mathbb{Z} : p = 4k+1, \\ \\ 2k+1, & \text{όταν } \exists k \in \mathbb{Z} : p = 4k+3, \end{cases}$$

οπότε *και* η δεύτερη εκ των ισοτήτων (5.91) είναι αληθής. □

5.7.18 Πρόταση. *Για κάθε πρώτον αριθμό $p \geq 3$ έχουμε*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)} = \begin{cases} 1, & \text{όταν } p \equiv \pm 1 (\mathrm{mod}\, 8), \\ \\ -1, & \text{όταν } p \equiv \pm 5 (\mathrm{mod}\, 8), \end{cases} \tag{5.92}$$

και

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \text{όταν } p \equiv 1 (\mathrm{mod}\, 8) \text{ ή } p \equiv -5 (\mathrm{mod}\, 8), \\ \\ -1, & \text{όταν } p \equiv 5 (\mathrm{mod}\, 8) \text{ ή } p \equiv -1 (\mathrm{mod}\, 8). \end{cases} \tag{5.93}$$

ΑΠΟΔΕΙΞΗ. Εδώ παρατίθεται μια σύντομη *δακτυλιοθεωρητική* απόδειξη. Αντί να εργασθούμε εντός τού $\mathbb{Z}$, θα εργασθούμε με τον δακτύλιο $\mathbb{Z}[i]$ των γκαουσιανών ακεραίων, εντός τού οποίου ο ακέραιος αριθμός 2 παραγοντοποιείται ως ακολούθως: $2=(-i)(1+i)^2$. Προφανώς,

$$2^{\frac{1}{2}(p-1)}=(-i)^{\frac{1}{2}(p-1)}(1+i)^{p-1}\Rightarrow 2^{\frac{1}{2}(p-1)}(1+i)=(-i)^{\frac{1}{2}(p-1)}(1+i)^p. \quad (5.94)$$

Εάν θεωρήσουμε την (5.94) "$\bmod p$" (το πραγματικό και το φανταστικό μέρος *χωριστά*) και λάβουμε υπ' όψιν ότι

$$\left.\begin{array}{r}(1+i)^p=\sum_{k=0}^{p}\binom{p}{k}i^k\\ p\mid\binom{p}{k},\ \forall k\in\{1,...,p-1\}\end{array}\right\}\Rightarrow (1+i)^p\equiv 1+i^p\,(\bmod p)\,,$$

τότε

$$2^{\frac{1}{2}(p-1)}(1+i)\equiv(-i)^{\frac{1}{2}(p-1)}(1+i^p)\,(\bmod p)\,. \quad (5.95)$$

Ο κάτωθι κατάλογος περιλαμβάνει τις τιμές τού δεξιού μέλους τής (5.95) συναρτήσει όλων των υπολοίπων που μπορεί να αφήνει το p διαιρούμενο διά τού 8.

p	$\frac{1}{2}(p-1)$	$(-i)^{\frac{1}{2}(p-1)}(1+i^p)$
$\equiv 1(\bmod 8)$	$\equiv 0(\bmod 4)$	$1+i$
$\equiv -5(\bmod 8)$	$\equiv 1(\bmod 4)$	$-1-i$
$\equiv 5(\bmod 8)$	$\equiv 2(\bmod 4)$	$-1-i$
$\equiv -1(\bmod 8)$	$\equiv 3(\bmod 4)$	$1+i$

Το $2^{\frac{1}{2}(p-1)}$ είναι $\equiv 1(\bmod p)$ όταν ισχύει $p\equiv\pm 1(\bmod 8)$ και $\equiv -1(\bmod p)$ όταν ισχύει $p\equiv\pm 5(\bmod 8)$, και αρκεί να εφαρμοσθεί το πόρισμα 5.7.16 για να συμπεράνουμε ότι το $\left(\frac{2}{p}\right)$ είναι αυτό που δίδεται από τον διπλό τύπο στην (5.92). Για την απόδειξη τής δεύτερης εκ των ισοτήτων (5.92) παρατηρούμε αρχικώς ότι αντικαθιστώντας τόν p με τον $p+8k$ ($k\in\mathbb{Z}$) στον εκθέτη λαμβάνουμε

$$(-1)^{\frac{(p+8k)^2-1}{8}}=(-1)^{\frac{p^2-1}{8}}\left((-1)^2\right)^{kp+4k^2}=(-1)^{\frac{p^2-1}{8}}\,,$$

οπότε το πρόσημο εξαρτάται μόνον από το υπόλοιπο που αφήνει το p διαιρούμενο διά τού 8. Εν συνεχεία, θέτοντας ± 1 και ± 5 στον εν λόγω εκθέτη εκτελούμε και τους τελευταίους απαραίτητους υπολογισμούς:

$$(-1)^{\frac{(\pm 1)^2-1}{8}}=(-1)^0=1\ \text{ και }\ (-1)^{\frac{(\pm 5)^2-1}{8}}=(-1)^3=-1.$$

Από την άλλη μεριά, σύμφωνα με το (iii) τής προτάσεως 5.7.17, την (5.91) και την (5.92), $\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{(p-1)(p+5)}{8}}$, οπότε η (5.93) είναι ωσαύτως αληθής[45]. □

[45] *Και* η τιμή τού εκθέτη $\frac{(p-1)(p+5)}{8}$ εξαρτάται μόνον από το εκάστοτε υπόλοιπο που αφήνει το p διαιρούμενο διά τού 8.

Για την περαιτέρω μελέτη και τον υπολογισμό των συμβόλων τού Legendre δεν είναι δυνατόν να αντιπαρέλθουμε τον λεγόμενο *νόμο τής τετραγωνικής αμοιβαιότητας* ή *τής αντιστροφής*, κάνοντας χρήση τού θεμελιώδους λήμματος 5.7.23. Ο Carl Friedrich Gauss (1777-1855) δημοσίευσε την *πρώτη ολοκληρωμένη* απόδειξη τού θεωρήματος 5.7.25 (που είχε διατυπωθεί ως εικασία *μερικώς* από τον P. Fermat και *πλήρως* από τους L. Euler[46] και A.-M. Legendre[47]) το έτος 1801 στο έργο του *Disquisitiones Arithmeticae* (έχοντάς την ανακαλύψει ήδη από την άνοιξη τού 1796). Από το 1801 έως το 1818 προσέθεσε άλλες 5 διαφορετικές αποδείξεις. Η συνηθέστερη (γεωμετρική-συνδυαστική) απόδειξη που συναντά κανείς στα σύγχρονα συγγράμματα Στοιχειώδους Θεωρίας Αριθμών είναι αυτή στην οποία υπεισέρχεται ο τύπος $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\kappa_1+\kappa_2}$ (ο προκύπτων από το λήμμα 5.7.23), όπου

$$\kappa_1 = \sum_{j=1}^{\frac{1}{2}(p-1)} \left\lfloor \tfrac{jq}{p} \right\rfloor \ \text{ και } \ \kappa_2 = \sum_{l=1}^{\frac{1}{2}(q-1)} \left\lfloor \tfrac{lp}{q} \right\rfloor,$$

ακολουθούμενος από κατάλληλη έκφραση των κ_1, κ_2 συναρτήσει τού πλήθους των κιγκλιδωματικών σημείων τού ορθογωνίου παραλληλογράμμου

$$\Pi := \left\{ (x,y) \in \mathbb{R}^2 \,\middle|\, 1 \le x \le \tfrac{1}{2}(p-1) \ \text{ και } \ 1 \le y \le \tfrac{1}{2}(q-1) \right\}$$

(τού έχοντος τα $(0,0), (\frac{p-1}{2}, 0), (0, \frac{q-1}{2})$ και $(\frac{p-1}{2}, \frac{q-1}{2})$ ως κορυφές του), από την οποία συνάγεται ότι

$$\mathrm{card}(\Pi \cap \mathbb{Z}^2) = \kappa_1 + \kappa_2 = \tfrac{(p-1)(q-1)}{4}.$$

Εδώ θα παρατεθεί μια κατά τι *συντομότερη* (τρόπον τινά *αναλυτική*) απόδειξη (τού 1845, με ελαφρά παραλλαγή τής πρωτότυπης), οφειλόμενη στον Gotthold Eisenstein[48] (1823-1852), η οποία βασίζεται στην κομψή τριγωνομετρική ταυτότητα (5.99) και σε απλούστατες ιδιότητες τής συναρτήσεως τού ημιτόνου.

5.7.19 Σημείωση. Έστω p ένας περιττός πρώτος αριθμός. Ένα *πλήρες σύστημα εκπροσώπων* τού $\mathbb{Z}$ ως προς τη σχέση ισοδυναμίας

$$a \sim_p b \underset{\text{ορσ}}{\iff} a \equiv b (\mathrm{mod}\, p) \ \ (\iff [a]_p = [b]_p)$$

(την οριζόμενη επί τού $\mathbb{Z}$) ή, απλούστερα, ένα *πλήρες σύστημα υπολοίπων*[49] $\bmod p$,

[46] L. Euler: *Theoremata circa divisores numerorum in hac forma* $pa^2 \pm qb^2$ contentorum, Comm. Acad. Sc. St. Petersburg **14** (1744-46), 151-181.

[47] Στο έργο του *Recherches d' Arithmetique* (1775) ο A.-M. Legendre διατυπώνει ένα θεώρημα ισοδύναμο τού 5.7.25, χωρίς να είναι σε θέση να δώσει λεπτομερή απόδειξη.

[48] G. Eisenstein: *Application de l'Algèbre à l'Arithmétique transcendante,* J. Reine Angew. Math. **29** (1845), 177-184.

[49] Προσοχή! Εδώ το *πλήρες σύστημα υπολοίπων* στην ορολογία χρησιμοποιείται υπό μία διευρυμένη έννοια. Βάσει τού θεωρήματος 5.1.1, κάθε ακέραιος διαιρούμενος διά τού p αφήνει *υπόλοιπο* ανήκον στο $\{0, 1, \ldots, p-1\}$. Ένα πλήρες σύστημα υπολοίπων σχηματίζεται επιλέγοντας p εκπροσώπους, *έναν* από εκάστη των κλάσεων ισοδυναμίας $[0]_p, [1]_p, \ldots, [p-1]_p$. Μια άλλη (*δακτυλιοθεωρητική*, αυτήν τη φορά) διεύρυνση τής κλασικής εννοίας τού *υπολοίπου* έχουμε ήδη συναντήσει στα εδάφια 5.4.2 (ii) και 5.4.19 (ii).

είναι ένα σύνολο p στοιχείων τής μορφής $\{l_0, l_1, ..., l_{p-1}\}$, όπου

$$l_j \in \mathbb{Z} \text{ και } l_j \equiv j (\mathrm{mod}\, p),\ \forall j \in \{0, 1, \dots, p-1\}.$$

Είναι προφανές ότι τα

$$\{0, 1, \dots, p-1\},\ \{1, \dots, p\} \text{ και } \{0, \pm 1, \dots, \pm \tfrac{p-1}{2}\} \tag{5.96}$$

αποτελούν τρία παραδείγματα πλήρων συστημάτων υπολοίπων $\mathrm{mod}\, p$. Οιοδήποτε μη κενό υποσύνολο ενός πλήρους συστήματος υπολοίπων $\mathrm{mod}\, p$ καλείται *μερικό σύστημα υπολοίπων* $\mathrm{mod}\, p$. Εδώ θα μας ασχολήσει ένα ειδικό σύστημα αυτού τού είδους. Συγκεκριμένα, το

$$\{\pm 1, \dots, \pm \tfrac{p-1}{2}\}, \tag{5.97}$$

το οποίο προκύπτει ύστερα από αφαίρεση τού 0 από το τρίτο εκ των πλήρων συστημάτων (5.96).

5.7.20 Λήμμα. *Εάν p είναι ένας περιττός πρώτος αριθμός και $a \in \mathbb{Z}$ με $p \nmid a$, τότε ο a, διαιρούμενος διά τού p, αφήνει υπόλοιπο (υπό την κλασική έννοια) που είναι ισότιμο ενός (και μόνον) στοιχείου l τού* (5.97) $\mathrm{mod}\, p$. *Μάλιστα, το $|l|$ ισούται με την ελάχιστη των απολύτων τιμών όλων των ακεραίων αριθμών που τυγχάνει να είναι* $\equiv a (\mathrm{mod}\, p)$.

ΑΠΟΔΕΙΞΗ. Ο ακέραιος a, διαιρούμενος διά τού p, αφήνει υπόλοιπο ανήκον στο σύνολο $\{1, 2, \dots, p-1\}$. Προφανώς,

$$\tfrac{1}{2}(p-1) + j \equiv -\tfrac{1}{2}(p-1) + j - 1 (\mathrm{mod}\, p),\ \forall j \in \{1, 2, \dots, \tfrac{p-1}{2}\},$$

οπότε κάθε στοιχείο τού συνόλου $\{1, 2, \dots, p-1\}$ είναι ισότιμο ενός (και μόνον) στοιχείου τού (5.97) $\mathrm{mod}\, p$. Εξάλλου, εάν $a \equiv l (\mathrm{mod}\, p)$, με τον l ανήκοντα στο (5.97), τότε $0 < |l| = \min\{|l'| : a \equiv l' (\mathrm{mod}\, p)\} \leq \frac{1}{2}(p-1) < p$ λόγω των προαναφερθέντων. □

5.7.21 Ορισμός. Το (5.97) γράφεται ως αποσυνδετή ένωση

$$S \coprod (-S) \text{ των } S := \{1, \dots, \tfrac{p-1}{2}\} \text{ και } -S := \{-s |\, s \in S\}$$

και χαρακτηρίζεται (λόγω τής ιδιότητας τής περιγραφείσας στο λήμμα 5.7.20) ως το **κατ' απόλυτη τιμή ελάχιστο σύστημα υπολοίπων** $\mathrm{mod}\, p$, το δε S ως το **σύνηθες ημίσειο σύστημα υπολοίπων** $\mathrm{mod}\, p$. Επιπροσθέτως, για κάθε παγιωμένον $a \in \mathbb{Z}$ με $p \nmid a$ και για κάθε $s \in S$ έχουμε $p \nmid sa$, οπότε (σύμφωνα με το λήμμα 5.7.20) υπάρχουν *μονοσημάντως ορισμένοι* ακέραιοι $\varepsilon_s(a) \in \{1, -1\}$ και $s_a \in S$, τέτοιοι ώστε να ισχύει

$$\boxed{sa \equiv \varepsilon_s(a) s_a (\mathrm{mod}\, p).}$$

5.7.22 Λήμμα. *Η απεικόνιση $S \ni s \longmapsto s_a \in S$ είναι αμφιρριπτική.*

ΑΠΟΔΕΙΞΗ. Επειδή το S είναι πεπερασμένο σύνολο, αρκεί να αποδειχθεί ότι η εν λόγω απεικόνιση είναι ενριπτική. Ας υποθέσουμε ότι $s, s' \in S$ είναι τέτοια, ώστε να ισχύει $s_a = s'_a$. Από τις ισοτιμίες

$$s_a \equiv \varepsilon_s(a)sa (\mathrm{mod}\, p) \;\; \text{και} \;\; s'_a \equiv \varepsilon_{s'}(a)s'a (\mathrm{mod}\, p)$$

έπεται ότι

$$\left.\begin{array}{r} s_a = s'_a \Rightarrow p \mid (\varepsilon_s(a)s - \varepsilon_{s'}(a)s')a \\ p \nmid a \end{array}\right\} \Rightarrow p \mid \varepsilon_s(a)s - \varepsilon_{s'}(a)s'.$$

Εξάλλου, επειδή $s, s' \in S$ και

$$|\varepsilon_s(a)s - \varepsilon_{s'}(a)s'| \leq |\varepsilon_s(a)s| + |\varepsilon_{s'}(a)s'| = s + s' \leq p - 1 < p,$$

έχουμε $\varepsilon_s(a)s - \varepsilon_{s'}(a)s' = 0 \Rightarrow (\varepsilon_s(a), \varepsilon_{s'}(a)) \in \{(1,1), (-1,-1)\}$ και $s = s'$. □

5.7.23 Λήμμα. («Λήμμα τού Gauss») *Εάν p είναι ένας περιττός πρώτος αριθμός και $a \in \mathbb{Z}$ με $p \nmid a$, τότε*

$$\boxed{\left(\tfrac{a}{p}\right) = \prod_{s \in S} \varepsilon_s(a) = (-1)^{\kappa},} \tag{5.98}$$

όπου κ είναι το πλήθος όσων εκ των $a, 2a, ..., \frac{p-1}{2}a$ είναι ισότιμοι $\mathrm{mod}\, p$ ενός στοιχείου τού $-S$.

ΑΠΟΔΕΙΞΗ. Από το λήμμα 5.7.22 έπεται ότι

$$\prod_{s \in S} sa \equiv \prod_{s \in S} \varepsilon_s(a)s_a = (\tfrac{1}{2}(p-1))! \prod_{s \in S} \varepsilon_s(a) (\mathrm{mod}\, p).$$

Επειδή $\prod\limits_{s \in S} sa = (\frac{1}{2}(p-1))!\, a^{\frac{p-1}{2}}$, έχουμε

$$\left.\begin{array}{r} p \mid (\frac{1}{2}(p-1))! \left(a^{\frac{p-1}{2}} - \prod\limits_{s \in S} \varepsilon_s(a) \right) \\ p \nmid (\frac{1}{2}(p-1))! \end{array}\right\} \Rightarrow a^{\frac{p-1}{2}} \equiv \prod_{s \in S} \varepsilon_s(a) (\mathrm{mod}\, p).$$

Όμως από το λήμμα 5.7.15 τού Euler, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p)$, οπότε

$$\left.\begin{array}{r} p \mid \left(\frac{a}{p}\right) - \prod\limits_{s \in S} \varepsilon_s(a) \in \{0, \pm 2\} \\ p \neq 2 \Rightarrow p \nmid \pm 2 \end{array}\right\} \Rightarrow \left(\tfrac{a}{p}\right) = \prod_{s \in S} \varepsilon_s(a).$$

Η δεύτερη εκ των ισοτήτων (5.98) είναι προφανής. □

5.7.24 Λήμμα. *Εάν k είναι ένας περιττός φυσικός αριθμός και $\nu = \frac{1}{2}(k-1)$, τότε για κάθε $x \in \mathbb{R}$ ισχύει η ακόλουθη τριγωνομετρική ταυτότητα*:

$$\boxed{\sin x = k \, \sin x/k \prod_{j=1}^{\nu} \left(1 - \frac{\sin^2 x/k}{\sin^2 j\pi/k}\right).} \tag{5.99}$$

ΑΠΟΔΕΙΞΗ. Από τον τύπο τού De Moivre $(\cos t + i \sin t)^k = \cos kt + i \sin kt$, $t \in \mathbb{R}$, λαμβάνουμε (ύστερα από διαχωρισμό τού φανταστικού μέρους από το πραγματικό)

$$\begin{aligned} \sin kt &= \sin t \left(\sum_{\varrho=0}^{\nu} (-1)^{\varrho} \binom{k}{2\varrho+1} \sin^{2\varrho} t \, \cos^{k-2\varrho-1} t \right) \\ &= \sin t \left(\sum_{\varrho=0}^{\nu} (-1)^{\varrho} \binom{k}{2\varrho+1} \sin^{2\varrho} t \, (1-\sin^2 t)^{\nu-\varrho} \right), \end{aligned}$$

οπότε το $\sin kt$ μπορεί να ιδωθεί ως «αποτίμηση»[50] τής πραγματικής πολυωνυμικής συναρτήσεως

$$\psi(u) := u \left(\sum_{\varrho=0}^{\nu} (-1)^{\varrho} \binom{k}{2\varrho+1} u^{2\varrho} (1-u^2)^{\nu-\varrho} \right)$$

(βαθμού k) στο $\sin t$. Επειδή $\sin kt = \psi(\sin t) = 0$ για τις k *σαφώς διακεκριμένες* τιμές $t = \frac{j\pi}{k}$, $j = 0, \pm 1, ..., \pm\nu$, υπάρχει σταθερά $c \in \mathbb{R}$, τέτοια ώστε να ισχύει

$$\sin kt = c \prod_{j=-\nu}^{\nu} \left(\sin t - \sin \frac{j\pi}{k} \right) = c \sin t \prod_{j \in \{\pm 1, ..., \pm\nu\}} \left(\sin t - \sin \frac{j\pi}{k} \right). \tag{5.100}$$

Προφανώς,

$$\begin{aligned} k &= \lim_{t \longrightarrow 0} \tfrac{1}{t} (\sin kt) = c \left(\lim_{t \longrightarrow 0} \tfrac{\sin t}{t} \right) \lim_{t \longrightarrow 0} \prod_{j \in \{\pm 1, ..., \pm\nu\}} \left(\sin t - \sin \tfrac{j\pi}{k} \right) \\ &= c \prod_{j \in \{\pm 1, ..., \pm\nu\}} \left(-\sin \tfrac{j\pi}{k} \right) = c \prod_{j \in \{\pm 1, ..., \pm\nu\}} \sin \tfrac{j\pi}{k} \Rightarrow c = \frac{k}{\prod_{j \in \{\pm 1, ..., \pm\nu\}} \sin \frac{j\pi}{k}}, \end{aligned}$$

διότι $\lim_{t \longrightarrow 0} \frac{\sin t}{t} = 1$. Θέτοντας x στη θέση τού kt η (5.100) γράφεται υπό τη μορφή

$$\begin{aligned} &\sin x = k \, \sin x/k \prod_{j \in \{\pm 1, ..., \pm\nu\}} \left(1 - \tfrac{\sin x/k}{\sin j\pi/k}\right) \\ &= k \, \sin x/k \prod_{j=1}^{\nu} \left(1 - \tfrac{\sin x/k}{\sin j\pi/k}\right) \left(1 + \tfrac{\sin x/k}{\sin j\pi/k}\right) \quad (\text{διότι } \sin(-y) = -\sin(y), \forall y \in \mathbb{R}) \\ &= k \, \sin x/k \prod_{j=1}^{\nu} \left(1 - \tfrac{\sin^2 x/k}{\sin^2 j\pi/k}\right), \end{aligned}$$

[50] Τα εισαγωγικά δηλούν το αυτονόητο: Σε ό,τι ακολουθεί εργαζόμαστε με τη σύνθεση $\psi \circ \sin$ και με το t ως μεταβλητή μας.

δίδοντάς μας την (5.99). □

5.7.25 Θεώρημα. (Νόμος τής «τετραγωνικής αμοιβαιότητας» ή «αντιστροφής») *Για οιουσδήποτε περιττούς πρώτους αριθμούς p και q με $p \neq q$ τα σύμβολα $\left(\frac{q}{p}\right)$ και $\left(\frac{p}{q}\right)$ τού Legendre συσχετίζονται μέσω τού τύπου*:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right), & \text{όταν } p \equiv q \equiv 3 (\mathrm{mod}\, 4), \\ \left(\frac{p}{q}\right), & \text{όταν } p \equiv 1 (\mathrm{mod}\, 4) \\ & \text{ή } q \equiv 1 (\mathrm{mod}\, 4) \end{cases} \tag{5.101}$$

ΑΠΟΔΕΙΞΗ. Εν πρώτοις θεωρούμε τα συνήθη ημίσεια συστήματα υπολοίπων ($\mathrm{mod}\, p$ και $\mathrm{mod}\, q$)

$$S := \{1, 2, ..., \tfrac{p-1}{2}\} \text{ και } T := \{1, 2, ..., \tfrac{q-1}{2}\}.$$

Για κάθε $s \in S$ υπάρχουν μονοσημάντως ορισμένα $\varepsilon_s(q) \in \{1, -1\}$ και $s_q \in S$ με $sq \equiv \varepsilon_s(q) s_q (\mathrm{mod}\, p)$. (Βλ. 5.7.22 και 5.7.21.) Επειδή η συνάρτηση τού ημιτόνου είναι περιττή και περιοδική, έχουσα περίοδο 2π, ισχύει

$$\sin \tfrac{2\pi}{p} sq = \sin \tfrac{2\pi}{p} \varepsilon_s(q) s_q = \varepsilon_s(q) \sin \tfrac{2\pi}{p} s_q \Rightarrow \varepsilon_s(q) = \frac{\sin \frac{2\pi}{p} sq}{\sin \frac{2\pi}{p} s_q}. \tag{5.102}$$

Πολλαπλασιάζοντας τις ισότητες (5.102) κατά μέλη για όλα τα $s \in S$ λαμβάνουμε (μέσω τής πρώτης εκ των ισοτήτων (5.98) τού λήμματος 5.7.23 τού Gauss και τής αμφιρριπτικότητας τής $S \ni s \longmapsto s_q \in S$ τής αποδειχθείσας στο λήμμα 5.7.22)

$$\left(\frac{q}{p}\right) = \prod_{s \in S} \varepsilon_s(a) = \prod_{s \in S} \frac{\sin \frac{2\pi}{p} sq}{\sin \frac{2\pi}{p} s_q} = \prod_{s \in S} \frac{\sin \frac{2\pi}{p} sq}{\sin \frac{2\pi}{p} s}. \tag{5.103}$$

Εν συνεχεία, θεωρούμε τυχόν $t \in T$, καθώς και τα μοναδικά $\varepsilon_t(2) \in \{1, -1\}$ και $t_2 \in T$, για τα οποία ισχύει $2t \equiv \varepsilon_t(2) t_2 (\mathrm{mod}\, p)$. Επειδή η συνάρτηση τού τετραγώνου τού ημιτόνου είναι άρτια και περιοδική, έχουσα περίοδο π, ισχύει

$$\sin^2 \tfrac{\pi}{q} 2t = \sin^2 \tfrac{\pi}{p} \varepsilon_t(2) t_2 = \sin^2 \tfrac{\pi}{p} t_2. \tag{5.104}$$

Χρησιμοποιώντας την τριγωνομετρική ταυτότητα (5.99) για $k := q, \nu := \frac{1}{2}(q-1)$ λαμβάνουμε (μέσω τής (5.104) και τού λήμματος 5.7.22 με το T στη θέση τού S)

$$\frac{\sin x}{\sin x/q} = q \prod_{j=1}^{\nu} \left(1 - \frac{\sin^2 x/q}{\sin^2 j\pi/q}\right) = q \prod_{t \in T} \left(1 - \frac{\sin^2 x/q}{\sin^2 t\pi/q}\right)$$

$$= q \prod_{t \in T} \left(1 - \frac{\sin^2 x/q}{\sin^2 t_2\pi/q}\right) = q \prod_{t \in T} \left(1 - \frac{\sin^2 x/q}{\sin^2 2t\pi/q}\right).$$

Κατόπιν εφαρμογής αυτών των ισοτήτων για $x = \frac{2\pi}{p}sq$ η (5.103) γράφεται ως

$$\left(\frac{q}{p}\right) = \prod_{s\in S} \frac{\sin\frac{2\pi}{p}sq}{\sin\frac{2\pi}{p}s} = \prod_{s\in S}\left(q\prod_{t\in T}\left(1-\frac{\sin^2 2\pi s/p}{\sin^2 2\pi t/q}\right)\right)$$

ή, ισοδυνάμως, ως

$$\boxed{\left(\frac{q}{p}\right) = q^{\frac{1}{2}(p-1)}\prod_{s\in S}\prod_{t\in T}\left(1-\frac{\sin^2 2\pi s/p}{\sin^2 2\pi t/q}\right).} \tag{5.105}$$

Με εναλλαγή των ρόλων των p και q και επανάληψη τής ίδιας διαδικασίας καταλήγουμε στην

$$\boxed{\left(\frac{p}{q}\right) = p^{\frac{1}{2}(q-1)}\prod_{s\in S}\prod_{t\in T}\left(1-\frac{\sin^2 2\pi t/q}{\sin^2 2\pi s/p}\right).} \tag{5.106}$$

Τα σύμβολα τού Legendre $\left(\frac{q}{p}\right)$ και $\left(\frac{p}{q}\right)$ είναι ίσα είτε με 1 είτε με -1, οπότε τα δεξιά μέλη των (5.105) και (5.106) είναι είτε ίσα είτε αντίθετα, και οι απόλυτες τιμές τους ίσες με 1. Επειδή λοιπόν διαφέρουν το πολύ ως προς το πρόσημό τους και $q^{\frac{1}{2}(p-1)} > 0$, $p^{\frac{1}{2}(q-1)} > 0$, αρκεί να εξετασθούν τα πρόσημα των διπλών γινόμενων. Προφανώς,

$$1-\frac{\sin^2 2\pi s/p}{\sin^2 2\pi t/q} > 0 \Longleftrightarrow 1-\frac{\sin^2 2\pi t/q}{\sin^2 2\pi s/p} < 0.$$

Τούτο, σε συνδυασμό με το ότι το πλήθος των διατεταγμένων ζευγών $(s,t)\in S\times T$ ισούται με $\mathrm{card}(S\times T) = \frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$, έχει ως επακόλουθο ότι το δεξιό (και, κατ' επέκταση, και το αριστερό) μέλος τής μίας εκ των (5.105), (5.106) αποκτάται από το δεξιό (και, κατ' επέκταση, και από το αριστερό) μέλος τής άλλης ύστερα από πολλαπλασιασμό του με το $(-1)^{\frac{(p-1)(q-1)}{4}}$. Η δεύτερη εκ των ισοτήτων (5.101) είναι προφανής. □

5.7.26 Σημείωση. (i) Μέχρι στιγμής είναι γνωστές περίπου 250 *διαφορετικές αποδείξεις* τού θεωρήματος 5.7.25, προερχόμενες από ποικίλους υποκλάδους τής Αλγεβρικής Θεωρίας Αριθμών, τής Θεωρίας Ομάδων, τής Θεωρίας Σωμάτων, τής Μιγαδικής Αναλύσεως κ.ά.[51]

(ii) Ο νόμος τής τετραγωνικής αμοιβαιότητας επιδέχεται σωρεία γενικεύσεων. Ο Erich Hecke (1887-1947) αναφέρει[52] σχετικώς: «Οι απαρχές τής σύγχρονης Αλγεβρικής Θεωρίας Αριθμών ανάγονται χρονικώς στην ανακάλυψη τού νόμου τής

[51] Πρβλ. F. Lemmermeyer: *Reciprocity Laws. From Euler to Eisenstein*, Springer-Verlag, 2000, καθώς και την ιστοσελίδα: http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html

[52] Βλ. E. Hecke: *Vorlesung über die Theorie der algebraischen Zahlen,* Akademische Verlagsgesellschaft, Leipzig 1923, σελ. 59-60.

τετραγωνικής αμοιβαιότητας. Παρότι αυτός εκ τής φύσεώς του ανήκει στη θεωρία των ρητών αριθμών, καθώς μπορεί να διατυπωθεί καθ' ολοκληρίαν ως απλός συσχετισμός μεταξύ κάποιων ρητών αριθμών, το περιεχόμενό του μας οδηγεί πολύ πέραν τής περιοχής των ρητών αριθμών. [...] Η εξέλιξη τής Αλγεβρικής Θεωρίας Αριθμών έχει πλέον όντως καταδείξει ότι το περιεχόμενο τού νόμου τής τετραγωνικής αμοιβαιότητας μπορεί να κατανοηθεί πλήρως μόνον όταν κανείς μεταβαίνει στους γενικούς *αλγεβρικούς αριθμούς* και ότι μια απόδειξη, η οποία προσήκει στην ουσία τού προβλήματος, οφείλει να χρησιμοποιεί αυτά τα προκεχωρημένα τεχνικά βοηθητικά μέσα· αντιθέτως, οι στοιχειώδεις αποδείξεις προσλαμβάνουν τον χαρακτήρα μιας *εκ των υστέρων* επαληθεύσεως.» Από την άλλη, όμως, πλευρά, το 1978 η Emma Lehmer (1906-2007) προσθέτει τα εξής[53]: «Είναι πασίγνωστο ότι ο νόμος τής τετραγωνικής αμοιβαιότητας τού Legendre, για τον οποίο υφίστανται πληθώρα[54] δημοσιευμένων αποδείξεων, έχει γενικευθεί με την πάροδο των ετών και σε αριθμητικά σώματα από πολλούς επιφανείς μαθηματικούς, από τον Gauss έως τον Artin, έχοντας πλέον καταστεί σχεδόν αγνώριστος.»

(iii) Έστω $m \neq -1$ ένας ακέραιος αριθμός στερούμενος τετραγώνων[55]. Εάν $q_1, ..., q_k$ είναι οι πρώτοι διαιρέτες του και p κάποιος πρώτος αριθμός με $p \notin \{q_1, ..., q_k\}$, τότε ένας *πρακτικός* τρόπος υπολογισμού[56] τού συμβόλου τού Legendre $\left(\frac{m}{p}\right)$ είναι ο ακόλουθος:

Βήμα πρώτο. Κατ' αρχάς, χρησιμοποιώντας τό (iii) τής προτάσεως 5.7.17 το εκφράζουμε υπό τη μορφή

$$\left(\frac{m}{p}\right) = \begin{cases} \left(\frac{\pm 1}{p}\right) \prod_{j=1}^{k} \left(\frac{q_j}{p}\right), & \text{όταν } m = \pm \prod_{j=1}^{k} q_j, \\ \\ \left(\frac{\pm 2}{p}\right) \prod_{j=1}^{k} \left(\frac{q_j}{p}\right), & \text{όταν } m = \pm 2 \prod_{j=1}^{k} q_j. \end{cases}$$

Τα $\left(\frac{\pm 1}{p}\right)$ και $\left(\frac{\pm 2}{p}\right)$ είναι υπολογίσιμα μέσω των (5.91), (5.92) και (5.93). Υπολείπεται ο υπολογισμός τού $\left(\frac{q_j}{p}\right)$ για κάθε $j \in \{1, ..., k\}$.

Βήμα δεύτερο. Εάν $q_j > p$, τότε γράφουμε τον q_j ως $q_j = r_j p + s_j$ για κάποιον $r_j \in \mathbb{Z}$ και $s_j \in \{\pm 1, ..., \pm \frac{p-1}{2}\}$. Προφανώς, $\left(\frac{q_j}{p}\right) = \left(\frac{s_j}{p}\right)$. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι ο s_j στερείται τετραγώνων. Εν συνεχεία, επαναλαμβάνουμε το πρώτο βήμα με το s_j στη θέση τού m. (Γράφουμε το s_j ως

[53] Βλ. εισαγωγή τού άρθρου τής E. Lehmer: *Rational reciprocity laws*, American Mathematical Monthly **85** (1978), 467-472.

[54] Στο πρωτότυπο παρατίθεται ο μέχρι τότε (κατά προσέγγιση) γνωστός αριθμός των δημοσιευμένων αποδείξεων.

[55] Τούτο δεν αποτελεί ουσιαστικό περιορισμό, διότι εάν $m = n^2 m'$, όπου ο m' στερείται τετραγώνων, τότε έχουμε $\left(\frac{m}{p}\right) = \left(\frac{m'}{p}\right)$ (λόγω των (ii) και (iii) τής προτάσεως 5.7.17).

[56] Για έναν εκλεπτυσμένο αλγόριθμο (γρήγορου!) υπολογισμού τού συμβόλου τού Legendre βλ. R.P. Brent & P. Zimmermann: *An* O(M(n) log n) *algorithm for the Jacobi symbol*, Proc. ANTS-IX, Lecture Notes in Computer Science **6197** (2010), 83-95.

γινόμενο κάποιων πρώτων και τού -1, αν τύχει να είναι αρνητικός, κ.ο.κ.) Άρα μέσω αυτού τού βήματος μπορούμε πάντοτε να αναχθούμε στην περίπτωση κατά την οποία $q_j < p$.

Βήμα τρίτο. Έστω ότι $q_j < p$. Επειδή (σύμφωνα με το θεώρημα 5.7.25)

$$\left(\tfrac{q_j}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\tfrac{p}{q_j}\right),$$

επαναλαμβάνουμε το δεύτερο βήμα εναλλάσοντας τους ρόλους των q_i και p κ.ο.κ. Κατ' αυτόν τον τρόπο το $\left(\frac{m}{p}\right)$ εκφράζεται ως γινόμενο τού -1 υψωθέντος σε κάποια ήδη υπολογισθείσα δύναμη και πεπερασμένου πλήθους συμβόλων τού Legendre *βαθμιαίως μειούμενων* πρώτων αριθμών. Απλό παράδειγμα:

$$\left(\tfrac{53909}{19}\right) = \left(\tfrac{31}{19}\right)\left(\tfrac{37}{19}\right)\left(\tfrac{41}{19}\right),$$

όπου

$$\left(\tfrac{31}{19}\right) = \left(\tfrac{12}{19}\right) = \left(\tfrac{2^2}{19}\right)\left(\tfrac{3}{19}\right) = \left(\tfrac{3}{19}\right) = -\left(\tfrac{1}{3}\right) = -1,$$

$$\left(\tfrac{37}{19}\right) = \left(\tfrac{18}{19}\right) = \left(\tfrac{2}{19}\right)\left(\tfrac{9}{19}\right) = -\left(\tfrac{9}{19}\right) = -\left(\tfrac{3^2}{19}\right) = -1,$$

$$\left(\tfrac{41}{19}\right) = \left(\tfrac{5}{19}\right) = \left(\tfrac{19}{5}\right) = \left(\tfrac{4}{5}\right) = \left(\tfrac{2^2}{5}\right) = 1,$$

οπότε $\left(\frac{53909}{19}\right) = 1$. Εναλλακτικώς, χωρίς την αρχική παραγοντοποίηση,

$$\left(\tfrac{53909}{19}\right) = \left(\tfrac{6}{19}\right) = \left(\tfrac{2}{19}\right)\left(\tfrac{3}{19}\right) = -\left(\tfrac{3}{19}\right) = \left(\tfrac{19}{3}\right) = \left(\tfrac{1}{3}\right) = 1,$$

καθόσον $53909 = 2837 \cdot 19 + 6$. Στις επόμενες προτάσεις υπολογίζονται τα σύμβολα Legendre $\left(\frac{m}{p}\right)$ για $m = \pm 3, \pm 5, \pm 6, \pm 7$ που απαιτούνται για το θεώρημα 5.7.31.

5.7.27 Πρόταση. *Για κάθε πρώτον αριθμό $p \geq 5$ έχουμε*

$$\left(\tfrac{3}{p}\right) = \begin{cases} 1, & \text{όταν } p \equiv \pm 1 (\mathrm{mod}\, 12), \\ -1, & \text{όταν } p \equiv \pm 5 (\mathrm{mod}\, 12), \end{cases} \tag{5.107}$$

και

$$\left(\tfrac{-3}{p}\right) = \begin{cases} 1, & \text{όταν } p \equiv 1 (\mathrm{mod}\, 6), \\ -1, & \text{όταν } p \equiv 5 (\mathrm{mod}\, 6). \end{cases} \tag{5.108}$$

ΑΠΟΔΕΙΞΗ. Επειδή (λόγω τής (5.101), των (i) και (iv) τής προτάσεως 5.7.17 και τής (5.92))

$$\left(\tfrac{3}{p}\right) = \begin{cases} -\left(\frac{p}{3}\right), & \text{όταν } p \equiv 3 (\mathrm{mod}\, 4), \\ \left(\frac{p}{3}\right), & \text{όταν } p \equiv 1 (\mathrm{mod}\, 4), \end{cases} \quad \text{και} \quad \left(\tfrac{p}{3}\right) = \begin{cases} 1, & \text{όταν } p \equiv 1 (\mathrm{mod}\, 3), \\ -1, & \text{όταν } p \equiv 2 (\mathrm{mod}\, 3), \end{cases}$$

έχουμε

$$\left(\tfrac{3}{p}\right)=1 \Leftrightarrow \begin{cases} \text{(i)} & p\equiv 3(\mathrm{mod}\,4) & \text{και} & p\equiv 2(\mathrm{mod}\,3), \\ & & \text{ή} & \\ \text{(ii)} & p\equiv 1(\mathrm{mod}\,4) & \text{και} & p\equiv 1(\mathrm{mod}\,3), \end{cases}$$

και, αντιστοίχως,

$$\left(\tfrac{3}{p}\right)=-1 \Leftrightarrow \begin{cases} \text{(iii)} & p\equiv 3(\mathrm{mod}\,4) & \text{και} & p\equiv 1(\mathrm{mod}\,3), \\ & & \text{ή} & \\ \text{(iv)} & p\equiv 1(\mathrm{mod}\,4) & \text{και} & p\equiv 2(\mathrm{mod}\,3). \end{cases}$$

Σύμφωνα με το θεώρημα[57] 3.4.10, καθένα εκ των συστημάτων (i)-(iv) των ανωτέρω δύο ισοτιμιών έχει ως (μοναδική κατά μόδιο $4\cdot 3=12$) λύση την ακόλουθη:

Σύστημα	p	Αιτιολόγηση
(i)	$\equiv 59\equiv -1(\mathrm{mod}\,12)$	$3\cdot 3^{\phi(4)}+2\cdot 4^{\phi(3)}=59$
(ii)	$\equiv 24\equiv 1(\mathrm{mod}\,12)$	$3^{\phi(4)}+4^{\phi(3)}=24$
(iii)	$\equiv 43\equiv -5(\mathrm{mod}\,12)$	$3\cdot 3^{\phi(4)}+4^{\phi(3)}=43$
(iv)	$\equiv 41\equiv 5(\mathrm{mod}\,12)$	$3^{\phi(4)}+2\cdot 4^{\phi(3)}=41$

Άρα η (5.107) είναι αληθής[58]. Από την άλλη μεριά, το (iii) και το (iv) τής προτάσεως 5.7.17 και η (5.101) δίδουν

$$\left(\tfrac{-3}{p}\right)=\left(\tfrac{-1}{p}\right)\left(\tfrac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\,(-1)^{\frac{p-1}{2}}\left(\tfrac{p}{3}\right)=(-1)^{p-1}\left(\tfrac{p}{3}\right)=\left(\tfrac{p}{3}\right),$$

οπότε η (5.108) είναι ωσαύτως αληθής (αφού $p\equiv 1(\mathrm{mod}\,2)$). □

5.7.28 Πρόταση. *Για κάθε περιττό πρώτον αριθμό $p\neq 5$ έχουμε*

$$\left(\tfrac{5}{p}\right)=\begin{cases} 1, & \text{όταν } p\equiv \pm 1 \text{ ή } \pm 9(\mathrm{mod}\,20), \\ -1, & \text{όταν } p\equiv \pm 3 \text{ ή } \pm 7(\mathrm{mod}\,20), \end{cases} \tag{5.109}$$

και

$$\left(\tfrac{-5}{p}\right)=\begin{cases} 1, & \text{όταν } p\equiv 1,3,7 \text{ ή } 9(\mathrm{mod}\,20), \\ -1, & \text{όταν } p\equiv -1,-3,-7 \text{ ή } -9(\mathrm{mod}\,20). \end{cases} \tag{5.110}$$

[57] Εάν μκδ$(m_1,m_2)=1$, τότε μέσω τού θεωρήματος 3.4.10 και τής (3.18) λαμβάνουμε

$$[p\equiv b_1(\mathrm{mod}\,m_1) \text{ και } p\equiv b_2(\mathrm{mod}\,m_2)] \Leftrightarrow p\equiv b_1 m_2^{\phi(m_1)}+b_2 m_1^{\phi(m_2)}(\mathrm{mod}\,m_1m_2).$$

[58] Σημειωτέον ότι κάθε αριθμός τής μορφής $12k\pm 1$ ή $12k\pm 5$ ($k\in\mathbb{Z}$) είναι *περιττός*, οπότε η ισοτιμία $p\equiv 1(\mathrm{mod}\,2)$ πληρούται *αυτομάτως* όταν πληρούται μία εκ των (5.107).

ΑΠΟΔΕΙΞΗ. Επειδή (λόγω τής (5.101), τού ότι $p \equiv \pm 1$ ή $\pm 2 (\mathrm{mod}\, 5)$, των (i) και (iv) τής προτάσεως 5.7.17 και των (5.92) και (5.93))

$$\left(\tfrac{5}{p}\right) = \left(\tfrac{p}{5}\right) = \begin{cases} 1, & \text{όταν } p \equiv \pm 1 (\mathrm{mod}\, 5), \\ \\ -1, & \text{όταν } p \equiv \pm 2 (\mathrm{mod}\, 5), \end{cases}$$

και (εξ υποθέσεως) $p \equiv \pm 1 (\mathrm{mod}\, 4)$, έχουμε

$$\left(\tfrac{5}{p}\right) = 1 \Leftrightarrow \begin{cases} \text{(i)} & p \equiv \pm 1 (\mathrm{mod}\, 4) & \text{και} & p \equiv \pm 1 (\mathrm{mod}\, 5), \\ & & \text{ή} & \\ \text{(ii)} & p \equiv \pm 1 (\mathrm{mod}\, 4) & \text{και} & p \equiv \mp 1 (\mathrm{mod}\, 5), \end{cases}$$

και, αντιστοίχως,

$$\left(\tfrac{5}{p}\right) = -1 \Leftrightarrow \begin{cases} \text{(iii)} & p \equiv \pm 1 (\mathrm{mod}\, 4) & \text{και} & p \equiv \pm 2 (\mathrm{mod}\, 5), \\ & & \text{ή} & \\ \text{(iv)} & p \equiv \pm 1 (\mathrm{mod}\, 4) & \text{και} & p \equiv \mp 2 (\mathrm{mod}\, 5). \end{cases}$$

Σύμφωνα με το θεώρημα 3.4.10, καθένα εκ των συστημάτων (i)-(iv) των ανωτέρω ζευγών ισοτιμιών έχει ως (μοναδική κατά μόδιο $4 \cdot 5 = 20$) λύση την ακόλουθη:

Σύστημα	p	Αιτιολόγηση
(i)	$\equiv \pm 281 \equiv \pm 1 (\mathrm{mod}\, 20)$	$\pm(5^{\phi(4)} + 4^{\phi(5)}) = \pm 281$
(ii)	$\equiv \mp 231 \equiv \pm 9 (\mathrm{mod}\, 20)$	$\pm(5^{\phi(4)} - 4^{\phi(5)}) = \mp 231$
(iii)	$\equiv \pm 537 \equiv \mp 3 (\mathrm{mod}\, 20)$	$\pm(5^{\phi(4)} + 2 \cdot 4^{\phi(5)}) = \pm 537$
(iv)	$\equiv \mp 487 \equiv \mp 7 (\mathrm{mod}\, 20)$	$\pm(5^{\phi(4)} - 2 \cdot 4^{\phi(5)}) = \mp 487$

Από την άλλη μεριά, τα (iii) και (iv) τής προτάσεως 5.7.17 δίδουν

$$\left(\tfrac{-5}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\tfrac{5}{p}\right),$$

οπότε η (5.110) είναι ωσαύτως αληθής (λόγω τής (5.109)). □

5.7.29 Πρόταση. *Για κάθε πρώτον αριθμό $p \geq 5$ έχουμε*

$$\left(\tfrac{6}{p}\right) = \begin{cases} 1, & \text{όταν } p \equiv \pm 1 \text{ ή } \pm 5 (\mathrm{mod}\ 24), \\ \\ -1, & \text{όταν } p \equiv \pm 7 \text{ ή } \pm 11 (\mathrm{mod}\ 24), \end{cases} \tag{5.111}$$

και

$$\left(\tfrac{-6}{p}\right) = \begin{cases} 1, & \text{όταν } p \equiv 1, 5, 7 \text{ ή } 11 (\mathrm{mod}\ 24), \\ \\ -1, & \text{όταν } p \equiv -1, -5, -7 \text{ ή } -11 (\mathrm{mod}\ 24). \end{cases} \tag{5.112}$$

ΑΠΟΔΕΙΞΗ. Επειδή $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$ (βλ. 5.7.17 (iii)), έχουμε

$$\left(\frac{6}{p}\right) = \begin{cases} 1, & \text{όταν } \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1 \text{ ή } \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1, \\ -1, & \text{όταν } \left[\left(\frac{2}{p}\right) = 1 \text{ και } \left(\frac{3}{p}\right) = -1\right] \text{ ή } \left[\left(\frac{2}{p}\right) = 1 \text{ και } \left(\frac{3}{p}\right) = -1\right]. \end{cases}$$

Ως εκ τούτου, οι (5.92) και (5.107) δίδουν

$$\left(\frac{6}{p}\right) = 1 \Leftrightarrow \begin{cases} \text{(i)} & p \equiv \pm 1 (\mathrm{mod}\, 8) & \text{και} & p \equiv \pm 1 (\mathrm{mod}\, 12), \\ & & \text{ή} & \\ \text{(ii)} & p \equiv \pm 5 (\mathrm{mod}\, 8) & \text{και} & p \equiv \pm 5 (\mathrm{mod}\, 12), \end{cases}$$

Επειδή $\mu\kappa\delta(8, 12) = 4$, το σύστημα (i) (και αντιστοίχως, το σύστημα (ii)) των ανωτέρω δύο ισοτιμιών είναι επιλύσιμο μόνον για τους συνδυασμούς προσήμων $+, +$ και $-, -$. Σύμφωνα με το θεώρημα 3.4.15, για καθέναν εξ αυτών των συνδυασμών το (i) (και αντιστοίχως, το (ii)) διαθέτει μία (και μόνον) λύση κατά μόδιο $\epsilon\kappa\pi(8, 12) = 24$. Απλοί υπολογισμοί μάς οδηγούν[59] στις 4 λύσεις:

Σύστημα	Πρόσημα	p
(i)	$+, +$	$\equiv 1 (\mathrm{mod}\, 24)$
(i)	$-, -$	$\equiv -1 (\mathrm{mod}\, 24)$
(ii)	$+, +$	$\equiv 5 (\mathrm{mod}\, 24)$
(ii)	$-, -$	$\equiv -5 (\mathrm{mod}\, 24)$

Κατ' αναλογίαν,

$$\left(\frac{6}{p}\right) = -1 \Leftrightarrow \begin{cases} \text{(i)} & p \equiv \pm 1 (\mathrm{mod}\, 8) & \text{και} & p \equiv \pm 5 (\mathrm{mod}\, 12), \\ & & \text{ή} & \\ \text{(ii)} & p \equiv \pm 5 (\mathrm{mod}\, 8) & \text{και} & p \equiv \pm 1 (\mathrm{mod}\, 12), \end{cases}$$

Το σύστημα (i) (και αντιστοίχως, το σύστημα (ii)) των ανωτέρω δύο ισοτιμιών είναι επιλύσιμο μόνον για τους συνδυασμούς προσήμων $+, +$ και $-, -$. Σύμφωνα με το θεώρημα 3.4.15, για καθέναν εξ αυτών των συνδυασμών το (i) (και αντιστοίχως, το (ii)) διαθέτει μία (και μόνον) λύση κατά μόδιο 24. Γράφοντας $4 = -4 \cdot 8 + 3 \cdot 12$, απλοί υπολογισμοί μάς οδηγούν στις 4 λύσεις:

Σύστημα	Πρόσημα	p
(i)	$+, +$	$\equiv -31 \equiv -7 (\mathrm{mod}\, 24)$
(i)	$-, -$	$\equiv 31 \equiv 7 (\mathrm{mod}\, 24)$
(ii)	$+, +$	$\equiv 37 \equiv -11 (\mathrm{mod}\, 24)$
(ii)	$-, -$	$\equiv -37 \equiv 11 (\mathrm{mod}\, 24)$

[59] Εάν $d := \mu\kappa\delta(m_1, m_2) \mid b_1 - b_2$ και εάν γράψουμε $d = k_1 m_1 + k_2 m_2$ για κατάλληλους $k_1, k_2 \in \mathbb{Z}$, τότε μέσω τού θεωρήματος 3.4.15 και των αναφερθέντων στην απόδειξη τού λήμματος 3.4.13 λαμβάνουμε

$$[p \equiv b_1 (\mathrm{mod}\, m_1) \text{ και } p \equiv b_2 (\mathrm{mod}\, m_2)] \Leftrightarrow p \equiv b_1 + \tfrac{m_1 k_1 (b_2 - b_1)}{d} (\mathrm{mod}\, \epsilon\kappa\pi(m_1, m_2)).$$

Από την άλλη μεριά, επειδή (λόγω των (iii) και (iv) τής προτάσεως 5.7.17)

$$\left(\tfrac{-6}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{6}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\tfrac{6}{p}\right),$$

η (5.112) προκύπτει άμεσα από την (5.111). □

5.7.30 Πρόταση. *Για κάθε περιττό πρώτον αριθμό $p \neq 7$ έχουμε*

$$\left(\tfrac{7}{p}\right) = \begin{cases} 1, & \text{όταν } p \equiv \pm 1, \pm 3 \text{ ή } \pm 9 (\mathrm{mod}\, 28), \\ -1, & \text{όταν } p \equiv \pm 5, \pm 11 \text{ ή } \pm 13 (\mathrm{mod}\, 28), \end{cases} \tag{5.113}$$

και

$$\left(\tfrac{-7}{p}\right) = \begin{cases} 1, & \text{όταν } p \equiv 1, -3, -5, 9, 11 \text{ ή } -13 (\mathrm{mod}\, 28), \\ -1, & \text{όταν } p \equiv -1, 3, 5, -9, -11 \text{ ή } 13 (\mathrm{mod}\, 28). \end{cases} \tag{5.114}$$

ΑΠΟΔΕΙΞΗ. Η (5.101) δίδει

$$\left(\tfrac{7}{p}\right) = \begin{cases} -\left(\tfrac{p}{7}\right), & \text{όταν } p \equiv 3 (\mathrm{mod}\, 4), \\ \left(\tfrac{p}{7}\right), & \text{όταν } p \equiv 1 (\mathrm{mod}\, 4). \end{cases} \tag{5.115}$$

Επειδή $p \equiv \pm 1, \pm 2$ ή $\pm 3 (\mathrm{mod}\, 7)$ και (λόγω των (5.91), (5.92), (5.93), (5.107) και (5.108)) ισχύει $\left(\tfrac{1}{7}\right) = \left(\tfrac{2}{7}\right) = \left(\tfrac{-3}{7}\right) = 1$, $\left(\tfrac{-1}{7}\right) = \left(\tfrac{-2}{7}\right) = \left(\tfrac{3}{7}\right) = -1$, από το (i) τής προτάσεως 5.7.17 και την (5.115) συνάγεται ότι $\left(\tfrac{7}{p}\right) = 1$ *εάν και μόνον εάν* ο p πληροί ένα εκ των κάτωθι έξι συστημάτων ζευγών γραμμικών ισοτιμιών:

$$\left\{ \begin{array}{llll} \text{(i)} & p \equiv -1 (\mathrm{mod}\, 7) & \text{και} & p \equiv 3 (\mathrm{mod}\, 4), \\ \text{(ii)} & p \equiv -2 (\mathrm{mod}\, 7) & \text{και} & p \equiv 3 (\mathrm{mod}\, 4), \\ \text{(iii)} & p \equiv 3 (\mathrm{mod}\, 7) & \text{και} & p \equiv 3 (\mathrm{mod}\, 4), \\ \text{(iv)} & p \equiv 1 (\mathrm{mod}\, 7) & \text{και} & p \equiv 1 (\mathrm{mod}\, 4), \\ \text{(v)} & p \equiv 2 (\mathrm{mod}\, 7) & \text{και} & p \equiv 1 (\mathrm{mod}\, 4), \\ \text{(vi)} & p \equiv -3 (\mathrm{mod}\, 7) & \text{και} & p \equiv 1 (\mathrm{mod}\, 4). \end{array} \right\}$$

Επειδή $(-1) \cdot 7 + 2 \cdot 4 = 1 = \text{μκδ}(7, 4)$ η (μοναδική κατά μόδιο $7 \cdot 4 = 28$) λύση καθενός εξ αυτών είναι η εξής[60]:

Σύστημα	$p \equiv ? \ (\mathrm{mod}\, 28)$	Σύστημα	$p \equiv ? \ (\mathrm{mod}\, 28)$
(i)	$-1 - 7(3 - (-1)) = -29 \equiv -1$	(iv)	$1 - 7(1 - 1) = 1$
(ii)	$-2 - 7(3 - (-2)) = -37 \equiv -9$	(v)	$2 - 7(1 - 2) = 9$
(iii)	$3 - 7(3 - 3) = 3$	(vi)	$-3 - 7(1 - (-3)) = -31 \equiv -3$

[60] Επειδή ο αριθμός $\phi(7) = 6$ είναι αρκετά μεγάλος ως εκθέτης, για την επίλυση των ανωτέρω συστημάτων προτιμήθηκε να ακολουθηθεί ό,τι έχει προαναφερθεί στην απόδειξη τού λήμματος 3.4.13.

Η περίπτωση κατά την οποία ισχύει $\left(\frac{7}{p}\right) = -1$ μπορεί να εξετασθεί παρομοίως[61]. Από την άλλη μεριά, τα (iii) και (iv) τής προτάσεως 5.7.17 δίδουν

$$\left(\tfrac{-7}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{7}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\tfrac{7}{p}\right),$$

οπότε η (5.114) είναι ωσαύτως αληθής (λόγω τής (5.113)). □

5.7.31 Θεώρημα. *Για έναν πρώτον αριθμό p ισχύουν τα εξής*:

(i) $\left[\exists x, y \in \mathbb{Z} : p = x^2 + y^2\right] \Leftrightarrow [\text{είτε } p = 2 \text{ είτε } p \equiv 1 (\mathrm{mod}\, 4)]$.

(ii) $\left[\exists x, y \in \mathbb{Z} : p = x^2 + 2y^2\right] \Leftrightarrow [\text{είτε } p = 2 \text{ είτε } p \equiv 1 \text{ ή } 3 (\mathrm{mod}\, 8)]$.

(iii) $\left[\exists x, y \in \mathbb{Z} : p = x^2 + xy + y^2\right] \Leftrightarrow [\text{είτε } p = 3 \text{ είτε } p \equiv 1 (\mathrm{mod}\, 6)]$.

(iv) $\left[\exists x, y \in \mathbb{Z} : p = x^2 + 3y^2\right] \Leftrightarrow [\text{είτε } p = 3 \text{ είτε } p \equiv 1 (\mathrm{mod}\, 6)]$.

(v) $\left[\exists x, y \in \mathbb{Z} : p = x^2 + 5y^2\right] \Rightarrow \left[\begin{array}{c}\text{είτε } p = 5 \text{ είτε} \\ p \equiv 1, 3, 7 \text{ ή } 9 (\mathrm{mod}\, 20)\end{array}\right]$.

(vi) $\left[\exists x, y \in \mathbb{Z} : p = x^2 + 6y^2\right] \Rightarrow [p \equiv 1, 5, 7 \text{ ή } 11 (\mathrm{mod}\, 24)]$.

(vii) $\left[\exists x, y \in \mathbb{Z} : p = x^2 + xy + 2y^2\right] \Leftrightarrow \left[\begin{array}{c}\text{είτε } p \in \{2, 7\} \text{ είτε} \\ p \equiv 1, 9, 11, 15, 23 \text{ ή } 25 (\mathrm{mod}\, 28)\end{array}\right]$.

(viii) $\left[\exists x, y \in \mathbb{Z} : p = \left|x^2 - 2y^2\right|\right] \Leftrightarrow [\text{είτε } p = 2 \text{ είτε } p \equiv \pm 1 (\mathrm{mod}\ 8)]$.

(ix) $\left[\exists x, y \in \mathbb{Z} : p = \left|x^2 - 3y^2\right|\right] \Leftrightarrow [\text{είτε } p = 3 \text{ είτε } p \equiv \pm 1 (\mathrm{mod}\, 12)]$.

(x) $\left[\exists x, y \in \mathbb{Z} : p = \left|x^2 + xy - y^2\right|\right] \Leftrightarrow \left[\begin{array}{c}\text{είτε } p = 5 \text{ είτε} \\ p \equiv \pm 1 \text{ ή } \pm 9 (\mathrm{mod}\, 20)\end{array}\right]$.

(xi) $\left[\exists x, y \in \mathbb{Z} : p = \left|x^2 - 6y^2\right|\right] \Leftrightarrow \left[\begin{array}{c}\text{είτε } p \in \{2, 3\} \text{ είτε} \\ p \equiv \pm 1 \text{ ή } \pm 5 (\mathrm{mod}\, 24)\end{array}\right]$.

(xii) $\left[\exists x, y \in \mathbb{Z} : p = \left|x^2 - 7y^2\right|\right] \Leftrightarrow \left[\begin{array}{c}\text{είτε } p \in \{2, 7\} \text{ είτε} \\ p \equiv \pm 1, \pm 3 \text{ ή } \pm 9 (\mathrm{mod}\, 28)\end{array}\right]$.

ΑΠΟΔΕΙΞΗ. (i) Όταν $p = 2$, έχουμε $2 = 1^2 + 1^2$. Όταν $p \neq 2$, η αμφίπλευρη συνεπαγωγή έπεται από το θεώρημα 5.7.3 ή, εναλλακτικώς, από την (5.86) για $m = -1$ και την (5.91).

(ii) Όταν $p = 2$, έχουμε $2 = 0^2 + 2 \cdot 1^2$. Όταν $p \neq 2$, η αμφίπλευρη συνεπαγωγή έπεται από την (5.86) για $m = -2$ και την (5.93).

(iii) Όταν $p = 3$, έχουμε $3 = 1^2 + 1 \cdot 1 + 1^2$. Όταν $p \neq 3$, η αμφίπλευρη συνεπαγωγή έπεται από την (5.87) για $m = -3$ και την (5.108).

(iv) Επειδή η $x^2 + 3y^2 = 2$ δεν διαθέτει ακέραιες λύσεις και $3 = 0^2 + 3 \cdot 1^2$, μπορούμε να υποθέσουμε ότι $p \geq 5$.

[61] Φυσικά, για να αποφύγει κανείς διπλό αριθμό πράξεων μπορεί να επιχειρηματολογήσει και ως ακολούθως: Επειδή *κάθε* περιττός πρώτος $p \neq 7$ διαιρούμενος διά τού 28 αφήνει υπόλοιπο $\pm 1, \pm 3, \pm 5, \pm 9, \pm 11$ ή ± 13 και $\left(\frac{7}{p}\right) = \pm 1$, και ο p οφείλει να υπόκειται σε ανάλογους περιορισμούς ακόμη και όταν $\left(\frac{7}{p}\right) = -1$ (με απλή εναλλαγή των $3 (\mathrm{mod}\, 4)$ και $1 (\mathrm{mod}\, 4)$), το ότι $\left(\frac{7}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 3$ ή $\pm 9 (\mathrm{mod}\, 28)$ σημαίνει *αυτομάτως* ότι $\left(\frac{7}{p}\right) = -1 \Leftrightarrow p \equiv \pm 5, \pm 11$ ή $\pm 13 (\mathrm{mod}\, 28)$.

"⇒" Εάν $p = x^2+3y^2$ για κάποιους $x, y \in \mathbb{Z}$, τότε $x^2 \equiv -3y^2 (\mathrm{mod}\, p)$, μκδ$(x,p) = 1$ και μκδ$(y,p) = 1$. Άρα υπάρχει $y' \in \mathbb{Z}$ με $yy' \equiv 1 (\mathrm{mod}\, p)$ και

$$\left.\begin{array}{r}(xy')^2 \equiv -3 (\mathrm{mod}\, p)\\ \text{μκδ}(xy', p) = 1\end{array}\right\} \Rightarrow \left(\tfrac{-3}{p}\right) = 1 \underset{(5.108)}{\Longrightarrow} p \equiv 1 (\mathrm{mod}\, 6).$$

"⇐" Ας υποθέσουμε ότι $p \equiv 1 (\mathrm{mod}\, 6)$. Τότε $\left(\frac{-3}{p}\right) = 1 \Rightarrow \exists \kappa \in \mathbb{Z} : \kappa^2 \equiv -3 (\mathrm{mod}\, p)$.

Θέτοντας $\lambda := \lfloor \sqrt{p} \rfloor$ έχουμε $\lambda < \sqrt{p} < \lambda + 1$. Θεωρούμε το σύνολο

$$\mathcal{A} := \{\, u + \kappa v |\, (u,v) \in \mathcal{B}\}\,, \text{ όπου } \mathcal{B} := \{\, (u,v) \in \mathbb{N}_0 \times \mathbb{N}_0 |\, u \le \lambda, v \le \lambda\}\,.$$

Επειδή $\mathrm{card}(\mathcal{B}) = (\lambda+1)^2 > p$, θα υπάρχουν $(u_1, v_1) \in \mathcal{B}$, $(u_2, v_2) \in \mathcal{B}$ με $(u_1, v_1) \neq (u_2, v_2)$, ούτως ώστε για τα στοιχεία $u_1 + \kappa v_1$ και $u_2 + \kappa v_2$ τού $\mathcal{A}$ να ισχύει

$$u_1 + \kappa v_1 \equiv u_2 + \kappa v_2 (\mathrm{mod}\, p) \Rightarrow u_1 - u_2 \equiv -\kappa (v_1 - v_2) (\mathrm{mod}\, p),$$

οπότε $a \equiv -\kappa b (\mathrm{mod}\, p)$, όπου $a := u_1 - v_1$ και $b := u_2 - v_2$ (με τουλάχιστον έναν εκ των a, b διάφορο τού μηδενός). Επομένως,

$$\left\{\begin{array}{c}\kappa^2 \equiv -3 (\mathrm{mod}\, p)\\ a \equiv -\kappa b (\mathrm{mod}\, p)\end{array}\right\} \Rightarrow \left\{\begin{array}{c}a^2 \equiv -3b^2 (\mathrm{mod}\, p)\\ \text{με } |a| \le \lambda \text{ και } |b| \le \lambda\end{array}\right\},$$

απ' όπου προκύπτει ότι

$$\left\{\begin{array}{c}0 < a^2 + 3b^2 \le 4\lambda^2 < 4p\\ p \mid a^2 + 3b^2\end{array}\right\} \Rightarrow a^2 + 3b^2 \in \{p, 2p, 3p\}.$$

Εάν $a^2 + 3b^2 = p$, τότε αρκεί να θέσουμε $x := a$ και $y := b$. Το ενδεχόμενο να ισχύει $a^2 + 3b^2 = 2p$ αποκλείεται, καθότι εν τοιαύτη περιπτώσει είτε αμφότεροι οι a, b θα ήταν άρτιοι είτε αμφότεροι οι a, b θα ήταν περιττοί και θα καταλήγαμε στην αναληθή ισοτιμία $2p \equiv 0 (\mathrm{mod}\, 4)$. Τέλος, εάν $a^2 + 3b^2 = 3p$, τότε $3 \mid a$ και $p = b^2 + 3(\frac{1}{3}a)^2$, οπότε αρκεί να θέσουμε $x := b$ και $y := \frac{1}{3}a$.

(v) Αυτή η *απλή* συνεπαγωγή είναι επακόλουθο τής (5.84) για $m = -5$, τής (5.110) και τού ότι $5 = 0^2 + 5 \cdot 1^2$.

(vi) Η εν λόγω *απλή* συνεπαγωγή έπεται από την (5.84) για $m = -6$ και την (5.112).

(vii) Δεδομένου ότι $2 = 0^2 + 0 \cdot 1 + 2 \cdot 1^2$ και $7 = 1^2 - 1 \cdot 2 + 2 \cdot 2^2$, τούτο προκύπτει από την (5.87) για $m = -7$ και την (5.114).

(viii) Αρκεί να εφαρμοσθεί η (5.86) για $m = 2$ σε συνδυασμό με την (5.92), λαμβανομένου υπ' όψιν ότι $2 = \left|0^2 - 2 \cdot 1^2\right|$.

(ix) Επειδή $3 = \left|0^2 - 3 \cdot 1^2\right|$, τούτο συνάγεται από την (5.86) για $m = 3$ και την (5.107).

(x) Έπεται άμεσα εφαρμόζοντας την (5.87) για $m = 5$ και την (5.109), δεδομένου ότι $5 = \left|3^2 + 3(-1) - (-1)^2\right|$.
(xi) Επειδή $2 = \left|2^2 - 6 \cdot 1^2\right|$, $3 = \left|3^2 - 6 \cdot 1^2\right|$, ο ισχυρισμός είναι αληθής επί τη βάσει τής (5.86) για $m = 6$ και τής (5.111).
(xii) Δεδομένου ότι $2 = \left|3^2 - 7 \cdot 1^2\right|$ και $7 = \left|0^2 - 7 \cdot 1^2\right|$, τούτο προκύπτει από την (5.86) για $m = 7$ και την (5.113). □

5.7.32 Σημείωση. Εάν $p \geq 5$, τότε από τις αμφίπλευρες συνεπαγωγές (iii) και (iv) τού θεωρήματος 5.7.31 παρατηρούμε ότι η συνθήκη $p \equiv 1 (\mathrm{mod}\, 6)$ ισοδυναμεί με το ότι ο p ισούται *τόσον* με την αριθμητική στάθμη ενός στοιχείου $x + y\sqrt{-3}$ (για κατάλληλους $x, y \in \mathbb{Z}$) τής Π.Μ.Π. $\mathfrak{O}_{-3}$ *όσον* και με την (διαφορετική!) αριθμητική στάθμη ενός στοιχείου $x + y\sqrt{-3}$ (για κατάλληλους $x, y \in \mathbb{Z}$) τής ακεραίας περιοχής $\mathbb{Z}[\sqrt{-3}] \subsetneqq \mathfrak{O}_{-3}$ *που δεν είναι* Π.Μ.Π.! Κατ' αναλογίαν, για έναν πρώτο αριθμό p αποδεικνύεται ότι

$$\left[\exists x, y \in \mathbb{Z} : p = x^2 + 7y^2\right] \Longleftrightarrow \left[\begin{array}{c} \text{είτε } p \in \{2, 7\} \text{ είτε} \\ p \equiv 1, 9, 11, 15, 23 \text{ ή } 25 (\mathrm{mod}\ 28) \end{array}\right].$$

Όμως τούτο δεν θα πρέπει να μας οδηγήσει σε εσφαλμένες γενικεύσεις. Επί παραδείγματι, επειδή οι $\mathfrak{O}_{-5} = \mathbb{Z}[\sqrt{-5}]$ και $\mathfrak{O}_{-6} = \mathbb{Z}[\sqrt{-6}]$ *δεν είναι* Π.Μ.Π. (και $-5 \not\equiv 1 (\mathrm{mod}\, 4)$, $-6 \not\equiv 1 (\mathrm{mod}\, 4)$), οι απλές συνεπαγωγές (v) και (vi) τού θεωρήματος 5.7.31 *δεν μπορούν* να αντιστραφούν απαράλλακτες. Στην πρώτη περίπτωση αποδεικνύεται[62] η αμφίπλευρη συνεπαγωγή

$$\left[\exists x, y \in \mathbb{Z} : p = x^2 + 5y^2\right] \Longleftrightarrow [\text{είτε } p = 5 \text{ είτε } p \equiv 1 \text{ ή } 9 (\mathrm{mod}\, 20)]$$

και στη δεύτερη περίπτωση η

$$\left[\exists x, y \in \mathbb{Z} : p = x^2 + 6y^2\right] \Longleftrightarrow [p \equiv 1 \text{ ή } 7 (\mathrm{mod}\ 24)]\,.$$

► **Αθροίσματα τριών τετραγώνων**. Η ικανή και αναγκαία συνθήκη προκειμένου ένας $n \in \mathbb{N}$ να εκφράζεται ως άθροισμα των τετραγώνων *τριών* ακεραίων αριθμών δίδεται στο θεώρημα 5.7.49. Η απόδειξη τής μίας κατευθύνσεως (ήτοι τής συνεπαγωγής (i)⇒(ii)) είναι εύκολη. Ωστόσο, η άλλη (η αντίστροφη συνεπαγωγή (ii)⇒(i)) είναι αρκετά περίπλοκη, κάτι που οφείλεται εν πολλοίς στο ότι η ιδιότητα τού να παριστάται ένας $n \in \mathbb{N}$ ως άθροισμα *τριών* τετραγώνων (εν αντιθέσει προς την περίπτωση των *δύο* τετραγώνων) *δεν είναι* πολλαπλασιαστική[63]. (Πρβλ. λήμμα 5.7.7.) Οι πρώτες αποδείξεις τού θεωρήματος 5.7.49 δημοσιεύθηκαν από τους A.-M. Legendre[64] (1798) και C.-F. Gauss[65] (1801). Υπάρχουν διαφορετικές

[62] Για τις δύο αμφίπλευρες συνεπαγωγές που ακολουθούν βλ. D.A. Cox: *Primes of the Form* $x^2 + ny^2$, 2nd ed., John Wiley & Sons, Inc., 2013, pp. 31-33.

[63] Επί παραδείγματι, ο αριθμός $8 \cdot 1 + 7 = 15 = (1^2 + 1^2 + 1^2)(2^2 + 1^2 + 0^2)$ δεν μπορεί να εκφρασθεί ως άθροισμα τριών τετραγώνων!

[64] A.-M. Legendre: *Essai sur la théorie des nombres*, Paris, An. **VI** (1797-1798), 398-399.

[65] *Disquisitiones Arithmeticae*, εδ. 291-292.

μέθοδοι αντιμετωπίσεως τού προβλήματος, όπως, π.χ., απευθείας μέσω τής διοφαντικής εξισώσεως τού Legendre, μέσω τού λήμματος των Davenport και Cassels[66], μέσω τού θεωρήματος περί κυρτών σωμάτων τού Minkowski[67], μέσω των τριαδικών ακεραίων τετραγωνικών μορφών κ.ά. Εδώ θα προτιμηθεί η πρόσβαση σε αυτό μέσω των τετραγωνικών μορφών που είναι μάλλον η στοιχειωδέστερη, αν και μακροσκελής, υπό την προϋπόθεση *τής χρήσεως και μόνον* τού περιώνυμου *θεωρήματος* 5.7.44 *τού Dirichlet* περί τής υπάρξεως άπειρων πρώτων μεταξύ των όρων *κατάλληλων αριθμητικών προόδων*, όπως προτάθηκε από τον E. Landau[68] το 1927.

5.7.33 Ορισμός. (i) Έστω $\nu \in \mathbb{N}$, $\nu \geq 2$, και έστω $\mathbf{A} = (a_{jk})_{1\leq j,k\leq \nu} \in \mathrm{Mat}_{\nu\times\nu}(\mathbb{Z})$ ένας *συμμετρικός* $\nu \times \nu$-πίνακας (ήτοι $\mathbf{A} = \mathbf{A}^\intercal$) έχων ως εγγραφές του ακεραίους αριθμούς. Λέμε ότι η απεικόνιση

$$F_{\mathbf{A}} : \mathbb{Z}^\nu \longrightarrow \mathbb{Z},\ (x_1, ..., x_\nu) = \mathbf{x} \longmapsto F_{\mathbf{A}}(\mathbf{x}) := \mathbf{x}\mathbf{A}\mathbf{x}^\intercal = \sum_{1\leq j,k\leq \nu} a_{jk}x_jx_k,$$

είναι **η ακεραία τετραγωνική μορφή η επαγόμενη μέσω τού $\mathbf{A}$**. Μια απεικόνιση $F : \mathbb{Z}^\nu \to \mathbb{Z}$ για την οποία υφίσταται συμμετρικός πίνακας $\mathbf{A} \in \mathrm{Mat}_{\nu\times\nu}(\mathbb{Z})$, ούτως ώστε να ισχύει $F = F_{\mathbf{A}}$, καλείται **ακεραία τετραγωνική μορφή ν μεταβλητών**. Οι ακέραιες τετραγωνικές μορφές ν μεταβλητών καλούνται, ιδιαιτέρως, **δυαδικές ακέραιες τετραγωνικές μορφές** όταν $\nu = 2$ και **τριαδικές ακέραιες τετραγωνικές μορφές** όταν $\nu = 3$.

(ii) Εάν $F = F_{\mathbf{A}}$, τότε η ορίζουσα $\mathrm{disc}(F) := \det(\mathbf{A})$ καλείται **διακρίνουσα** τής F.

(iii) Εάν $F_1 = F_{\mathbf{A}}$ και $F_2 = F_{\mathbf{B}}$ (αμφότερες ν μεταβλητών), τότε λέμε ότι οι F_1 και F_2 είναι **ισοδύναμες** και σημειώνουμε

$$F_1 \underset{\text{τ.μ.}}{\sim} F_2 \underset{\text{ορσ}}{\Longleftrightarrow} [\exists \mathbf{U} \in \mathrm{SL}_\nu(\mathbb{Z}) : \mathbf{B} = \mathbf{U}\mathbf{A}\mathbf{U}^\intercal],$$

όπου $\mathrm{SL}_\nu(\mathbb{Z}) := \{\mathbf{C} \in \mathrm{Mat}_{\nu\times\nu}(\mathbb{Z}) | \det(\mathbf{C}) = 1\}$. Είναι άμεσος ο έλεγχος τού ότι η "$\underset{\text{τ.μ.}}{\sim}$" είναι μια σχέση ισοδυναμίας, καθώς και τού ότι οι διακρίνουσες δυο ισοδυνάμων ακεραίων τετραγωνικών μορφών είναι ίσες.

(iv) Λέμε ότι ένας $n \in \mathbb{Z}$ είναι **παραστάσιμος** μέσω μιας ακεραίας τετραγωνικής μορφής $F : \mathbb{Z}^\nu \longrightarrow \mathbb{Z}$ όταν υπάρχει $\mathbf{x} \in \mathbb{Z}^\nu$, ούτως ώστε να ισχύει $n = F(\mathbf{x})$. Εάν ένας $n \in \mathbb{Z}$ είναι παραστάσιμος μέσω μιας $F_1 = F_{\mathbf{A}}$ και $F_1 \underset{\text{τ.μ.}}{\sim} F_2 = F_{\mathbf{B}}$, τότε αυτός είναι παραστάσιμος και μέσω τής F_2, διότι $\exists \mathbf{U} \in \mathrm{SL}_\nu(\mathbb{Z}) : \mathbf{A} = \mathbf{U}\mathbf{B}\mathbf{U}^\intercal$, οπότε (για κατάλληλο $\mathbf{x} \in \mathbb{Z}^\nu$ και $\mathbf{y} := \mathbf{x}\mathbf{U}$) έχουμε

$$n = F_{\mathbf{A}}(\mathbf{x}) = \mathbf{x}\mathbf{A}\mathbf{x}^\intercal = \mathbf{x}\mathbf{U}\mathbf{B}\mathbf{U}^\intercal\mathbf{x}^\intercal = \mathbf{y}\mathbf{B}\mathbf{y}^\intercal = F_{\mathbf{B}}(\mathbf{y}).$$

[66] J.-P. Serre: *A Course in Arithmetic*, G.T.M. Vol. **7**, Springer-Verlag, 1973, pp. 45-47.

[67] N.C. Ankeny: *Sums of three squares*, Proc. of the American Math. Society **8** (1957), 316-319.

[68] E. Landau: *Vorlesungen über Zahlentheorie*, Band I, Hirzel, Leibzig, 1927.

(v) Μια ακεραία τετραγωνική μορφή $F : \mathbb{Z}^\nu \longrightarrow \mathbb{Z}$ καλείται **θετικώς ορισμένη** όταν $F(\mathbf{x}) \geq 1$ για κάθε $\mathbf{x} \in \mathbb{Z}^\nu \smallsetminus \{(0, ..., 0)\}$. Σημειωτέον ότι κάθε ακεραία τετραγωνική μορφή, η οποία είναι ισοδύναμη με μια θετικώς ορισμένη ακεραία τετραγωνική μορφή, είναι θετικώς ορισμένη.

5.7.34 Λήμμα. *Εάν* $\mathbf{A} = (a_{jk})_{1\leq j,k\leq 2} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z})$ *είναι ένας συμμετρικός πίνακας, τότε τα ακόλουθα είναι ισοδύναμα* :

(i) *Η* $F_{\mathbf{A}}$ *είναι θετικώς ορισμένη.*

(ii) $a_{11} > 0$ *και* $\det(\mathbf{A}) = a_{11}a_{22} - a_{12}^2 > 0$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Ας υποθέσουμε ότι η

$$(x_1, x_2) \longmapsto F_{\mathbf{A}}(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2$$

είναι θετικώς ορισμένη. Τότε είναι πρόδηλο ότι $a_{11} = F_{\mathbf{A}}(1, 0)$ και

$$\begin{aligned} a_{11}\det(\mathbf{A}) &= a_{11}(a_{11}a_{22} - a_{12}^2) = a_{11}a_{12}^2 - 2a_{11}a_{12}^2 + a_{11}^2a_{22} \\ &= F_{\mathbf{A}}(-a_{12}, a_{11}) \geq 1 \Rightarrow \det(\mathbf{A}) = a_{11}a_{22} - a_{12}^2 \geq 1. \end{aligned}$$

(ii)⇒(i) Εάν $a_{11} \geq 1$ και $a_{11}a_{22} - a_{12}^2 \geq 1$, τότε

$$a_{11}F_{\mathbf{A}}(x_1, x_2) = (a_{11}x_1 + a_{12}x_2)^2 + \det(\mathbf{A})x_2^2 \geq 0$$

με $F_{\mathbf{A}}(x_1, x_2) = 0 \Leftrightarrow (x_1, x_2) = (0, 0)$. □

5.7.35 Λήμμα. *Η κλάση ισοδυναμίας* (*ως προς την* "$\underset{\text{τ.μ.}}{\sim}$") *οιασδήποτε θετικώς ορισμένης δυαδικής ακεραίας τετραγωνικής μορφής* F *με διακρίνουσα* d *διαθέτει ως εκπρόσωπό της* (*τουλάχιστον*) *μια τετραγωνική μορφή*

$$F_{\mathbf{A}}(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2, \text{ όπου } 2\,|a_{12}| \leq a_{11} \leq \tfrac{2}{\sqrt{3}}\sqrt{d}.$$

ΑΠΟΔΕΙΞΗ. $F = F_{\mathbf{B}}$ για κάποιον συμμετρικό $\mathbf{B} = (b_{jk})_{1\leq j,k\leq 2} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z})$. Θέτουμε

$$a_{11} := \min\left\{ l \in \mathbb{N} |\, \exists (x_1, x_2) \in \mathbb{Z}^2 : l = F_{\mathbf{B}}(x_1, x_2) \right\}.$$

Προφανώς, $a_{11} = F_{\mathbf{B}}(r_1, r_2)$ για κάποιο ζεύγος $(r_1, r_2) \in \mathbb{Z}^2$. Μάλιστα, μκδ$(r_1, r_2) = 1$, διότι εάν μκδ$(r_1, r_2) > 1$, τότε θα είχαμε

$$a_{11} \leq F_{\mathbf{B}}(\tfrac{r_1}{\text{μκδ}(r_1,r_2)}, \tfrac{r_2}{\text{μκδ}(r_1,r_2)}) = \tfrac{F_{\mathbf{B}}(r_1,r_2)}{\text{μκδ}(r_1,r_2)^2} = \tfrac{a_{11}}{\text{μκδ}(r_1,r_2)^2} < a_{11},$$

κάτι που είναι αδύνατο. Άρα υπάρχουν $s_1, s_2 \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει

$$1 = r_1s_2 - r_2s_1 = r_1(s_2 + r_2t) - r_2(s_1 + r_1t),\ \forall t \in \mathbb{Z}.$$

Για κάθε $t \in \mathbb{Z}$ θεωρούμε τον πίνακα

$$\mathbf{U}_t := \begin{pmatrix} r_1 & r_2 \\ s_1 + r_1 t & s_2 + r_2 t \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Θέτοντας $c_{12} := b_{11} r_1 s_1 + b_{12}(r_1 s_2 + r_2 s_1) + b_{22} r_2 s_2$ λαμβάνουμε

$$\mathbf{U}_t \mathbf{B} \mathbf{U}_t^{\intercal} = \begin{pmatrix} F_{\mathbf{B}}(r_1, r_2) & c_{12} + F_{\mathbf{B}}(r_1, r_2)t \\ c_{12} + F_{\mathbf{B}}(r_1, r_2)t & F_{\mathbf{B}}(s_1 + r_1 t, s_2 + r_2 t) \end{pmatrix},$$

όπου $F_{\mathbf{B}}(s_1 + r_1 t, s_2 + r_2 t) \geq F_{\mathbf{B}}(r_1, r_2)$, διότι $(s_1 + r_1 t, s_2 + r_2 t) \neq (0, 0)$. Εν συνεχεία, επιλέγοντας μια *συγκεκριμένη* ακεραία τιμή $t = t_0$ με

$$-\tfrac{1}{2} - \tfrac{c_{12}}{a_{11}} \leq t_0 \leq \tfrac{1}{2} - \tfrac{c_{12}}{a_{11}} \tag{5.116}$$

και θέτοντας

$$\mathbf{A} := \mathbf{U}_{t_0} \mathbf{B} \mathbf{U}_{t_0}^{\intercal} = \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}, \text{ όπου } a_{12} = c_{12} + a_{11} t_0$$

και $a_{22} = F_{\mathbf{B}}(s_1 + r_1 t_0, s_2 + r_2 t_0)$, παρατηρούμε ότι $F = F_{\mathbf{B}} \underset{\text{τ.μ.}}{\sim} F_{\mathbf{A}}$ με $|a_{12}| \leq \frac{a_{11}}{2}$ (λόγω τής (5.116)) και

$$\left.\begin{aligned} d = a_{11} a_{22} - a_{12}^2 \\ a_{22} \geq a_{11} \end{aligned}\right\} \Rightarrow a_{11}^2 \leq a_{11} a_{22} = d + a_{12}^2 \leq d + \tfrac{a_{11}^2}{4},$$

απ' όπου έπεται ότι $\frac{3a_{11}^2}{4} \leq d \Rightarrow a_{11} \leq \frac{2}{\sqrt{3}} \sqrt{d}$. □

5.7.36 Πρόταση. *Κάθε θετικώς ορισμένη δυαδική ακεραία τετραγωνική μορφή F με διακρίνουσα $d = 1$ είναι ισοδύναμη με την $(x_1, x_2) \longmapsto x_1^2 + x_2^2$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το λήμμα 5.7.35, $F \underset{\text{τ.μ.}}{\sim} F_{\mathbf{A}}$, όπου

$$F_{\mathbf{A}}(x_1, x_2) = a_{11} x_1^2 + 2 a_{12} x_1 x_2 + a_{22} x_2^2$$

με $2\,|a_{12}| \leq a_{11} \leq \frac{2}{\sqrt{3}} < 2$. Το λήμμα 5.7.34 μας πληροφορεί ότι $a_{11} \geq 1$, οπότε $a_{11} = 1$, $a_{12} = 0$. Εξ υποθέσεως, $1 = d = a_{11} a_{22} - a_{12}^2 = a_{22}$. Άρα ο ισχυρισμός είναι αληθής. □

5.7.37 Λήμμα. *Εάν $\mathbf{A} = (a_{jk})_{1 \leq j,k \leq 3} \in \mathrm{Mat}_{3\times 3}(\mathbb{Z})$ είναι ένας συμμετρικός πίνακας, τότε για την τριαδική ακεραία τετραγωνική μορφή $F_{\mathbf{A}}$ με διακρίνουσα d ισχύουν τα εξής*:

(i) *Για κάθε $(x_1, x_2, x_3) \in \mathbb{Z}^3$,*

$$a_{11} F_{\mathbf{A}}(x_1, x_2, x_3) = (a_{11} x_1 + a_{12} x_2 + a_{13} x_3)^2 + G_{\widehat{\mathbf{A}}}(x_2, x_3), \tag{5.117}$$

όπου $(x_2, x_3) \longmapsto G_{\widehat{\mathbf{A}}}(x_2, x_3)$ *είναι η δυαδική ακεραία τετραγωνική μορφή η επαγόμενη μέσω τού πίνακα*

$$\widehat{\mathbf{A}} := \begin{pmatrix} a_{11}a_{22} - a_{12}^2 & a_{11}a_{23} - a_{12}a_{13} \\ a_{11}a_{23} - a_{12}a_{13} & a_{11}a_{33} - a_{13}^2 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z})$$

με $\mathrm{disc}(G_{\widehat{\mathbf{A}}}) = \det(\widehat{\mathbf{A}}) = a_{11}d$.

(ii) *Εάν η* $F_{\mathbf{A}}$ *είναι θετικώς ορισμένη, τότε και η* $G_{\widehat{\mathbf{A}}}$ *είναι θετικώς ορισμένη.*

(iii) *Η* $F_{\mathbf{A}}$ *είναι θετικώς ορισμένη εάν και μόνον εάν*

$$a_{11} \geq 1,\ a_{11}a_{22} - a_{12}^2 \geq 1 \text{ και } d \geq 1.$$

ΑΠΟΔΕΙΞΗ. (i) Για κάθε $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$ έχουμε

$$\begin{aligned} a_{11}F_{\mathbf{A}}(x_1, x_2, x_3) &= a_{11}\left(\mathbf{x}\mathbf{A}\mathbf{x}^{\intercal}\right) \\ &= a_{11}\left(a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + 2a_{12}x_1x_2 + 2a_{23}x_2x_3 + 2a_{13}x_1x_3\right) \end{aligned}$$

και

$$\begin{aligned} G_{\widehat{\mathbf{A}}}(x_2, x_3) &= (x_2\ x_3)\begin{pmatrix} a_{11}a_{22} - a_{12}^2 & a_{11}a_{23} - a_{12}a_{13} \\ a_{11}a_{23} - a_{12}a_{13} & a_{11}a_{33} - a_{13}^2 \end{pmatrix}\begin{pmatrix} x_2 \\ x_3 \end{pmatrix} \\ &= \left(a_{11}a_{22} - a_{12}^2\right)x_2^2 + 2\left(a_{11}a_{23} - a_{12}a_{13}\right)x_2x_3 + \left(a_{11}a_{33} - a_{13}^2\right)x_3^2, \end{aligned}$$

και η (5.117) προκύπτει ύστερα από άμεσο υπολογισμό. Εξάλλου,

$$\begin{aligned} &d = a_{11}a_{22}a_{33} - a_{11}a_{23}^2 - a_{12}^2a_{33} + 2a_{12}a_{13}a_{23} - a_{13}^2a_{22} \\ &\Rightarrow a_{11}d = \det\begin{pmatrix} a_{11}a_{22} - a_{12}^2 & a_{11}a_{23} - a_{12}a_{13} \\ a_{11}a_{23} - a_{12}a_{13} & a_{11}a_{33} - a_{13}^2 \end{pmatrix}. \end{aligned}$$

(ii) Εάν η $F_{\mathbf{A}}$ είναι θετικώς ορισμένη, τότε $a_{11} = F_{\mathbf{A}}(1, 0, 0) \geq 1$ και εάν υποθέσουμε ότι $G_{\widehat{\mathbf{A}}}(x_2, x_3) \leq 0$ για κάποιους $x_2, x_3 \in \mathbb{Z}$, τότε ισχύει προφανώς $G_{\widehat{\mathbf{A}}}(a_{11}x_2, a_{11}x_3) = a_{11}G_{\widehat{\mathbf{A}}}(x_2, x_3) \leq 0$. Θέτοντας $x_1 := -(a_{12}x_2 + a_{13}x_3)$ λαμβάνουμε $a_{11}x_1 + a_{12}a_{11}x_2 + a_{13}a_{11}x_3 = 0$. Ως εκ τούτου,

$$\underbrace{a_{11}}_{\geq 1}\underbrace{F_{\mathbf{A}}(x_1, a_{11}x_2, a_{11}x_3)}_{\text{θετικώς ορισμένη}} \underset{(5.117)}{=} 0^2 + G_{\widehat{\mathbf{A}}}(a_{11}x_2, a_{11}x_3) \leq 0,$$

απ' όπου έπεται ότι $x_2 = x_3 = 0$, οπότε *και* η $G_{\widehat{\mathbf{A}}}$ είναι θετικώς ορισμένη.

(iii) "⇒" Εάν η τετραγωνική μορφή $F_{\mathbf{A}}$ είναι θετικώς ορισμένη, τότε (όπως είδαμε στο (ii)) $a_{11} \geq 1$. Εφαρμόζοντας το λήμμα 5.7.34 για τη θετικώς ορισμένη $G_{\widehat{\mathbf{A}}}$ λαμβάνουμε $a_{11}a_{22} - a_{12}^2 \geq 1$ και $\mathrm{disc}(G_{\widehat{\mathbf{A}}}) = a_{11}d \geq 1 \Rightarrow d \geq 1$.

"⇐" Από αυτές τις ανισοϊσότητες έπεται ότι η $G_{\widehat{\mathbf{A}}}$ είναι θετικώς ορισμένη (μέσω τού λήμματος 5.7.34). Επίσης, λόγω τής (5.117), $F_{\mathbf{A}}(x_1, x_2, x_3) \geq 0$ για κάθε

$(x_1, x_2, x_3) \in \mathbb{Z}^3$. Τέλος, εάν $F_{\mathbf{A}}(x_1, x_2, x_3) = 0$ για κάποιο $(x_1, x_2, x_3) \in \mathbb{Z}^3$, η (5.117) δίδει

$$\left.\begin{aligned} G_{\widehat{\mathbf{A}}}(x_2, x_3) = 0 \Rightarrow x_2 = x_3 = 0 \\ a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = 0 \end{aligned}\right\} \Rightarrow a_{11}x_1 = 0 \Rightarrow x_1 = 0,$$

οπότε $(x_1, x_2, x_3) = (0, 0, 0)$ και η $F_{\mathbf{A}}$ είναι όντως θετικώς ορισμένη. □

5.7.38 Σημείωση. Βάσει τού (i) τού λήμματος 5.7.37 σε κάθε τριαδική ακεραία τετραγωνική μορφή $F_{\mathbf{A}}$ αντιστοιχεί μια *μονοσημάντως ορισμένη* δυαδική ακεραία τετραγωνική μορφή $G_{\widehat{\mathbf{A}}}$. Μάλιστα, όπως θα δούμε στο αμέσως επόμενο λήμμα, σε κάθε στοιχείο ενός *ειδικού* συνόλου $\left\{ F_{\mathbf{A}_{r,s}} \middle| r, s \in \mathbb{Z} \right\}$ τριαδικών ακεραίων τετραγωνικών μορφών (παραμετρούμενου μέσω δυο ακεραίων r και s) με $F_{\mathbf{A}_{r,s}} \underset{\text{τ.μ.}}{\sim} F_{\mathbf{B}}$ (ήτοι με τις $F_{\mathbf{A}_{r,s}}$ ανήκουσες στην ίδια κλάση ισοδυναμίας) αντιστοιχεί η *ίδια* δυαδική ακεραία τετραγωνική μορφή.

5.7.39 Λήμμα. *Έστω ότι* $\mathbf{B} = (b_{jk})_{1 \le j,k \le 3} \in \mathrm{Mat}_{3\times 3}(\mathbb{Z})$ *είναι ένας συμμετρικός πίνακας, τέτοιος ώστε η* $(y_1, y_2, y_3) \longmapsto F_{\mathbf{B}}(y_1, y_2, y_3)$ *να είναι θετικώς ορισμένη και* $(y_2, y_3) \longmapsto G_{\widehat{\mathbf{B}}}(y_2, y_3)$ *η αντιστοιχούσα θετικώς ορισμένη δυαδική ακεραία τετραγωνική μορφή με*

$$b_{11}F_{\mathbf{B}}(y_1, y_2, y_3) = (b_{11}y_1 + b_{12}y_2 + b_{13}y_3)^2 + G_{\widehat{\mathbf{B}}}(y_2, y_3)$$

όπως στο λήμμα 5.7.37. *Εάν*

$$\widetilde{\mathbf{V}} = \begin{pmatrix} \widetilde{v}_{11} & \widetilde{v}_{12} \\ \widetilde{v}_{21} & \widetilde{v}_{22} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad \widetilde{\mathbf{A}} := \widetilde{\mathbf{V}}\,\widehat{\mathbf{B}}\,\widetilde{\mathbf{V}}^{\intercal},$$

$G_{\widetilde{\mathbf{A}}}$ ($\underset{\text{τ.μ.}}{\sim} G_{\widehat{\mathbf{B}}}$) *η δυαδική ακεραία τετραγωνική μορφή η επαγόμενη μέσω τού* $\widetilde{\mathbf{A}}$ *και για* $r, s \in \mathbb{Z}$,

$$\mathbf{V}_{r,s} := (v_{jk})_{1 \le j,k \le 3} := \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline r & \multicolumn{2}{c}{\multirow{2}{*}{$\widetilde{\mathbf{V}}$}} \\ s & & \end{array}\right) \in \mathrm{SL}_3(\mathbb{Z})$$

και $\mathbf{A}_{r,s} := (a_{jk})_{1 \le j,k \le 3} := \mathbf{V}_{r,s}\mathbf{B}\mathbf{V}_{r,s}^{\intercal}$ (*με τα* a_{jk} *εξαρτώμενα από τα* r, s), *τότε* $a_{11} = b_{11}$,

$$a_{11}F_{\mathbf{A}_{r,s}}(x_1, x_2, x_3) = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + G_{\widetilde{\mathbf{A}}}(x_2, x_3)$$

και $G_{\widetilde{\mathbf{A}}} = G_{\widehat{\mathbf{A}_{r,s}}}$ (*όπου η* $G_{\widehat{\mathbf{A}_{r,s}}}$ *είναι η δυαδική ακεραία τετραγωνική μορφή που αντιστοιχεί στην* $F_{\mathbf{A}_{r,s}}$ *όπως στο λήμμα* 5.7.37 *και η* $G_{\widetilde{\mathbf{A}}}$ *είναι ανεξάρτητη των* r, s).

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως, $v_{11} = 1, v_{12} = v_{13} = 0$. Εάν για $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$ θέσουμε $\mathbf{y} = (y_1, y_2, y_3) := \mathbf{x}\,\mathbf{V}_{r,s}, \widetilde{\mathbf{x}} := (x_2, x_3), \widetilde{\mathbf{y}} = (y_2, y_3) := \widetilde{\mathbf{x}}\,\widetilde{\mathbf{V}}$, τότε

$$y_1 = v_{11}x_1 + v_{21}x_2 + v_{31}x_3 = x_1 + rx_2 + sx_3,$$

$$y_2 = v_{12}x_1 + v_{22}x_2 + v_{32}x_3 = \widetilde{v}_{11}x_2 + \widetilde{v}_{21}x_3,$$

$$y_3 = v_{13}x_1 + v_{23}x_2 + v_{33}x_3 = \widetilde{v}_{12}x_2 + \widetilde{v}_{22}x_3,$$

και

$$G_{\widetilde{\mathbf{A}}}(x_2,x_3)=G_{\widetilde{\mathbf{A}}}(\widetilde{\mathbf{x}})=\widetilde{\mathbf{x}}\,\widetilde{\mathbf{A}}\,\widetilde{\mathbf{x}}^{\intercal}=\widetilde{\mathbf{y}}\,\widetilde{\mathbf{B}}\,\widetilde{\mathbf{y}}^{\intercal}=G_{\widehat{\mathbf{B}}}(\widetilde{\mathbf{y}})=G_{\widehat{\mathbf{B}}}(y_2,y_3),$$
$$F_{\mathbf{A}_{r,s}}(x_1,x_2,x_3)=F_{\mathbf{A}_{r,s}}(\mathbf{x})=\mathbf{x}\mathbf{A}_{r,s}\mathbf{x}^{\intercal}=\mathbf{y}\mathbf{B}\mathbf{y}^{\intercal}=F_{\mathbf{B}}(\mathbf{y})=F_{\mathbf{B}}(y_1,y_2,y_3).$$

Εξάλλου, επειδή

$$\begin{pmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{pmatrix}=\begin{pmatrix} 1 & 0 & 0\\ r & \widetilde{v}_{11} & \widetilde{v}_{12}\\ s & \widetilde{v}_{21} & \widetilde{v}_{22}\end{pmatrix}\begin{pmatrix} b_{11} & b_{12} & b_{13}\\ b_{12} & b_{22} & b_{23}\\ b_{13} & b_{23} & b_{33}\end{pmatrix}\begin{pmatrix} 1 & r & s\\ 0 & \widetilde{v}_{11} & \widetilde{v}_{21}\\ 0 & \widetilde{v}_{12} & \widetilde{v}_{22}\end{pmatrix},$$

έχουμε $a_{11}=b_{11}$ και

$$\begin{aligned} b_{11}y_1+b_{12}y_2+b_{13}y_3&=(y_1,y_2,y_3)\begin{pmatrix} b_{11}\\ b_{12}\\ b_{13}\end{pmatrix}\\ &=(x_1,x_2,x_3)\mathbf{V}_{r,s}\begin{pmatrix} b_{11}\\ b_{12}\\ b_{13}\end{pmatrix}=(x_1,x_2,x_3)\begin{pmatrix} b_{11}\\ rb_{11}+\widetilde{v}_{11}b_{12}+\widetilde{v}_{12}b_{13}\\ sb_{11}+\widetilde{v}_{21}b_{12}+\widetilde{v}_{22}b_{13}\end{pmatrix}\\ &=a_{11}x_1+a_{12}x_2+a_{13}x_3.\end{aligned}$$

Κατά συνέπειαν,

$$\begin{aligned}&(a_{11}x_1+a_{12}x_2+a_{13}x_3)^2+G_{\widehat{\mathbf{A}_{r,s}}}(x_2,x_3)=a_{11}F_{\mathbf{A}_{r,s}}(x_1,x_2,x_3)\\ &=b_{11}F_{\mathbf{B}}(y_1,y_2,y_3)=(b_{11}y_1+b_{12}y_2+b_{13}y_3)^2+G_{\widehat{\mathbf{B}}}(y_2,y_3)\\ &=(a_{11}x_1+a_{12}x_2+a_{13}x_3)^2+G_{\widetilde{\mathbf{A}}}(x_2,x_3),\end{aligned}$$

απ' όπου έπεται ότι $G_{\widehat{\mathbf{A}_{r,s}}}(x_2,x_3)=G_{\widetilde{\mathbf{A}}}(x_2,x_3)$ για κάθε ζεύγος $(x_2,x_3)\in\mathbb{Z}^2$. □

5.7.40 Λήμμα. *Εάν u_{11},u_{21} και u_{31} είναι τρεις ακέραιοι που είναι μεταξύ τους πρώτοι, τότε υφίστανται έξι ακέραιοι αριθμοί u_{jk}, $j\in\{1,2,3\}$, $k\in\{2,3\}$, τέτοιοι ώστε ο πίνακας $\mathbf{U}:=(u_{jk})_{1\le j,k\le 3}$ να έχει ορίζουσα ίση με 1.*

ΑΠΟΔΕΙΞΗ. Ως γνωστόν, ο μέγιστος κοινός διαιρέτης των u_{11} και u_{21} είναι ένας ακέραιος γραμμικός συνδυασμός αυτών. Άρα υπάρχουν $u_{12},u_{22}\in\mathbb{Z}$ με

$$u_{11}u_{22}-u_{21}u_{12}=\text{μκδ}(u_{11},u_{21}).$$

Επειδή δε $\text{μκδ}(\text{μκδ}(u_{11},u_{21}),u_{31})=\text{μκδ}(u_{11},u_{21},u_{31})=1$, υπάρχουν (για τον ίδιον λόγο) $u_{33},\xi\in\mathbb{Z}$ με

$$\text{μκδ}(u_{11},u_{21})u_{33}-\xi u_{31}=1.$$

Θέτοντας $u_{13}:=\frac{u_{11}\xi}{\text{μκδ}(u_{11},u_{21})}$, $u_{23}:=\frac{u_{21}\xi}{\text{μκδ}(u_{11},u_{21})}$, $u_{32}:=0$, βλέπουμε ότι ο πίνακας

$$\mathbf{U}:=\begin{pmatrix} u_{11} & u_{12} & u_{13}\\ u_{21} & u_{22} & u_{23}\\ u_{31} & u_{32} & u_{33}\end{pmatrix}=\begin{pmatrix} u_{11} & u_{12} & \frac{1}{\text{μκδ}(u_{11},u_{21})}u_{11}\xi\\ u_{21} & u_{22} & \frac{1}{\text{μκδ}(u_{11},u_{21})}u_{21}\xi\\ u_{31} & 0 & u_{33}\end{pmatrix}$$

έχει ορίζουσα

$$\begin{aligned}\det(\mathbf{U}) &= u_{31}(\tfrac{\xi}{\text{μκδ}(u_{11},u_{21})}(u_{21}u_{12}-u_{11}u_{22}))+u_{33}(u_{11}u_{22}-u_{21}u_{12})\\ &= -\xi u_{31}+u_{33}\text{μκδ}(u_{11},u_{21})=1.\end{aligned}$$ □

5.7.41 Λήμμα. *Η κλάση ισοδυναμίας (ως προς την "$\underset{\text{τ.μ.}}{\sim}$") οιασδήποτε θετικώς ορισμένης τριαδικής ακεραίας τετραγωνικής μορφής F με διακρίνουσα d διαθέτει ως εκπρόσωπό της (τουλάχιστον) μια τετραγωνική μορφή*

$$(x_1,x_2,x_3)\overset{F_{\mathbf{A}}}{\longmapsto}\sum_{1\le j,k\le 3}a_{jk}x_jx_k,\ \text{όπου}\ \ 2\max\{|a_{12}|,|a_{13}|\}\le a_{11}\le\tfrac{4}{3}\sqrt[3]{d}.$$

ΑΠΟΔΕΙΞΗ. Εξ ορισμού, $F=F_{\mathbf{C}}$ για κάποιον συμμετρικό πίνακα $\mathbf{C}\in\text{Mat}_{3\times 3}(\mathbb{Z})$. Θέτουμε

$$a_{11}:=\min\left\{F(x_1,x_2,x_3)|\,(x_1,x_2,x_3)\in\mathbb{Z}^3\smallsetminus\{(0,0,0)\}\right\}.$$

Προφανώς, $a_{11}=F(u_{11},u_{21},u_{31})$ για κατάλληλη διατεταγμένη τριάδα $(u_{11},u_{21},u_{31})\in\mathbb{Z}^3\smallsetminus\{(0,0,0)$. Μάλιστα, ισχύει $\text{μκδ}(u_{11},u_{21},u_{31})=1$, διότι εάν $\text{μκδ}(u_{11},u_{21},u_{31})>1$, τότε θα είχαμε

$$F(\tfrac{u_{11}}{\text{μκδ}(u_{11},u_{21},u_{31})},\tfrac{u_{21}}{\text{μκδ}(u_{11},u_{21},u_{31})},\tfrac{u_{31}}{\text{μκδ}(u_{11},u_{21},u_{31})})=\tfrac{a_{11}}{\text{μκδ}(u_{11},u_{21},u_{31})^2}<a_{11},$$

ήτοι κάτι το αδύνατο. Κατά το λήμμα 5.7.40 υπάρχουν $u_{jk}\in\mathbb{Z}$, $j\in\{1,2,3\}$, $k\in\{2,3\}$, με $\mathbf{U}:=(u_{jk})_{1\le j,k\le 3}\in\text{SL}_3(\mathbb{Z})$. Θέτουμε $\mathbf{B}:=(b_{jk})_{1\le j,k\le 3}:=\mathbf{UCU}^{\intercal}$. Προφανώς, $F=F_{\mathbf{C}}\underset{\text{τ.μ.}}{\sim}F_{\mathbf{B}}$, η $F_{\mathbf{B}}$ είναι θετικώς ορισμένη και ο $a_{11}=b_{11}$ είναι ο ελάχιστος φυσικός αριθμός που είναι παραστάσιμος *και* μέσω τής $F_{\mathbf{B}}$. Κατά το λήμμα 5.7.37,

$$a_{11}F_{\mathbf{B}}(x_1,x_2,x_3)=(b_{11}x_1+b_{12}x_2+b_{13}x_3)^2+G_{\widehat{\mathbf{B}}}(x_2,x_3),$$

όπου η $(x_2,x_3)\longmapsto G_{\widehat{\mathbf{B}}}(x_2,x_3)$ είναι η θετικώς ορισμένη δυαδική ακεραία τετραγωνική μορφή (με διακρίνουσα ίση με $a_{11}d$) που αντιστοιχεί στην $F_{\mathbf{B}}$. Το λήμμα 5.7.35 μας πληροφορεί ότι $G_{\widehat{\mathbf{B}}}\underset{\text{τ.μ.}}{\sim}G_{\widetilde{\mathbf{A}}}$, όπου η

$$(x_2,x_3)\longmapsto G_{\widetilde{\mathbf{A}}}(x_2,x_3)=\widetilde{a}_{11}x_2^2+2\widetilde{a}_{12}x_2x_3+\widetilde{a}_{22}x_3^2$$

είναι μια θετικώς ορισμένη δυαδική ακεραία τετραγωνική μορφή, επαγόμενη μέσω κάποιου συμμετρικού πίνακα $\widetilde{\mathbf{A}}=(\widetilde{a}_{jk})_{1\le j,k\le 2}\in\text{Mat}_{2\times 2}(\mathbb{Z})$ με $\widetilde{a}_{11}\le\frac{2}{\sqrt{3}}\sqrt{a_{11}d}$. Προφανώς,

$$\exists\,\widetilde{\mathbf{V}}=\begin{pmatrix}\widetilde{v}_{11}&\widetilde{v}_{12}\\ \widetilde{v}_{21}&\widetilde{v}_{22}\end{pmatrix}\in\text{SL}_2(\mathbb{Z}):\widetilde{\mathbf{A}}=\widetilde{\mathbf{V}}\,\widehat{\mathbf{B}}\,\widetilde{\mathbf{V}}^{\intercal}.$$

Εάν για οιουσδήποτε $r,s\in\mathbb{Z}$ θέσουμε

$$\mathbf{V}_{r,s}:=(v_{jk})_{1\le j,k\le 3}:=\left(\begin{array}{c|cc}1&0&0\\ r&\multicolumn{2}{c}{\multirow{2}{*}{$\widetilde{\mathbf{V}}$}}\\ s&&\end{array}\right)\in\text{SL}_3(\mathbb{Z})$$

και $\mathbf{A}_{r,s} := (a_{jk})_{1\le j,k\le 3} = \mathbf{V}_{r,s}\mathbf{B}\mathbf{V}_{r,s}^{\intercal}$ (όπως στο λήμμα 5.7.39, με τα a_{jk} εξαρτώμενα από τα r, s), τότε ο $\mathbf{A}_{r,s}$ είναι συμμετρικός, $G_{\widetilde{\mathbf{A}}} = G_{\widehat{\mathbf{A}_{r,s}}}$, $a_{11}a_{22} - a_{12}^2 = \widetilde{a}_{11}$ και

$$a_{12} = a_{21} = r\underbrace{b_{11}}_{=a_{11}} + \widetilde{v}_{11}b_{12} + \widetilde{v}_{12}b_{13},\ a_{13} = a_{31} = s\underbrace{b_{11}}_{=a_{11}} + \widetilde{v}_{21}b_{12} + \widetilde{v}_{22}b_{13}.$$

Επιλέγοντας μια *συγκεκριμένη* ακεραία τιμή $r = r_0$ με

$$-\tfrac{1}{2} - \tfrac{b_{12}}{a_{11}}\widetilde{v}_{11} - \tfrac{b_{13}}{a_{11}}\widetilde{v}_{12} \le r_0 \le \tfrac{1}{2} - \tfrac{b_{12}}{a_{11}}\widetilde{v}_{11} - \tfrac{b_{13}}{a_{11}}\widetilde{v}_{12}, \tag{5.118}$$

καθώς και μια *συγκεκριμένη* ακεραία τιμή $s = s_0$ με

$$-\tfrac{1}{2} - \tfrac{b_{12}}{a_{11}}\widetilde{v}_{21} - \tfrac{b_{13}}{a_{11}}\widetilde{v}_{22} \le s_0 \le \tfrac{1}{2} - \tfrac{b_{12}}{a_{11}}\widetilde{v}_{21} - \tfrac{b_{13}}{a_{11}}\widetilde{v}_{22}, \tag{5.119}$$

και θέτοντας $\mathbf{A} := \mathbf{A}_{r_0,s_0}$, παρατηρούμε ότι $F_{\mathbf{A}} \underset{\text{τ.μ.}}{\sim} F_{\mathbf{B}} \underset{\text{τ.μ.}}{\sim} F_{\mathbf{C}}$, ότι (λόγω των (5.118) και (5.119)) ισχύει

$$\left[|a_{12}| \le \tfrac{a_{11}}{2} \text{ και } |a_{13}| \le \tfrac{a_{11}}{2}\right] \Rightarrow 2\max\{|a_{12}|, |a_{13}|\} \le a_{11}$$

και, τέλος, ότι $a_{11} \le F_{\mathbf{A}}(0,1,0) = a_{22}$ (από τον τρόπο ορισμού τού a_{11}) και

$$\begin{aligned} &a_{11}^2 \le a_{11}a_{22} = \widetilde{a}_{11} + a_{12}^2 \le \tfrac{2}{\sqrt{3}}\sqrt{a_{11}d} + \tfrac{a_{11}^2}{4} \\ &\Rightarrow \tfrac{3}{4}a_{11}^{\frac{3}{2}} \le \tfrac{2}{\sqrt{3}}d^{\frac{1}{2}} \Rightarrow a_{11}^3 \le \tfrac{4^3}{3^3}d, \end{aligned}$$

απ' όπου συμπεραίνουμε ότι $a_{11} \le \frac{4}{3}\sqrt[3]{d}$. □

5.7.42 Πρόταση. *Κάθε θετικώς ορισμένη τριαδική ακεραία τετραγωνική μορφή F με διακρίνουσα $d = 1$ είναι ισοδύναμη με την $(x_1, x_2, x_3) \longmapsto x_1^2 + x_2^2 + x_3^2$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το λήμμα 5.7.41, $F \underset{\text{τ.μ.}}{\sim} F_{\mathbf{A}}$, όπου $d = \det(\mathbf{A}) = 1$ και

$$F_{\mathbf{A}}(x_1, x_2, x_3) = \sum_{1\le j,k\le 3} a_{jk}x_jx_k, \quad \max\{|a_{12}|, |a_{13}|\} \le \tfrac{a_{11}}{2} \le \tfrac{2}{3} < 1.$$

Επομένως, $a_{12} = a_{13} = 0$ και $d = 1 \Rightarrow a_{11} \ne 0 \Rightarrow a_{11} = 1$, απ' όπου έπεται ότι

$$\mathbf{A} = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{$\widehat{\mathbf{A}}$}} \\ 0 & & \end{array}\right) \Rightarrow d = \det(\widehat{\mathbf{A}}) = 1, \text{ όπου } \widehat{\mathbf{A}} := \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix}.$$

Η δυαδική ακεραία τετραγωνική μορφή $(x_2, x_3) \longmapsto G_{\widehat{\mathbf{A}}}(x_2, x_3)$ η επαγόμενη μέσω τού πίνακα $\widehat{\mathbf{A}}$ είναι θετικώς ορισμένη και *ταυτίζεται* με εκείνην που αντιστοιχεί στην $F_{\mathbf{A}}$. (Βλ. το (ii) τού λήμματος 5.7.37.) Κάτά την πρόταση 5.7.36,

$$\exists\, \widehat{\mathbf{U}} := \begin{pmatrix} u_{22} & u_{23} \\ u_{32} & u_{33} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \widehat{\mathbf{U}}\,\widehat{\mathbf{A}}\,\widehat{\mathbf{U}}^{\intercal} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Κατά συνέπειαν,

$$\mathbf{UAU}^{\intercal} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ όπου } \mathbf{U} := \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{$\widehat{\mathbf{U}}$}} \\ 0 & & \end{array}\right),$$

και ο ισχυρισμός είναι αληθής. □

5.7.43 Πόρισμα. *Έστω $m \in \mathbb{N}, m \geq 2$. Εάν για κάποιον $\kappa \in \mathbb{N}$ ο $-\kappa$ είναι τετραγωνικό ισοϋπόλοιπο κατά μόδιο $\kappa m - 1$* (βλ. εδ. 5.7.12)*, τότε ο m είναι παραστάσιμος ως άθροισμα των τετραγώνων τριών ακεραίων αριθμών.*

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως, $\exists a_{12}, a_{11} \in \mathbb{Z} : a_{12}^2 + \kappa = a_{11}(\kappa m - 1) = a_{11}a_{22}$, όπου $a_{22} := \kappa m - 1$ με

$$\left.\begin{aligned} a_{22} \geq 2\kappa - 1 \geq 1 \\ a_{11}a_{22} = a_{12}^2 + \kappa \geq \kappa \geq 1 \end{aligned}\right\} \Rightarrow a_{11} \geq 1,$$

$a_{11}a_{22} - a_{12}^2 \geq 1$ και $(a_{11}a_{22} - a_{12}^2)m - a_{22} = \kappa m - a_{22} = 1$. Το 5.7.37 (iii) μας πληροφορεί ότι η τριαδική ακεραία τετραγωνική μορφή $F_{\mathbf{A}}$ η επαγόμενη από τον πίνακα

$$\mathbf{A} := \left(\begin{array}{cc|c} a_{11} & a_{12} & 1 \\ a_{12} & a_{22} & 0 \\ \hline 1 & 0 & m \end{array}\right) \in \mathrm{SL}_3(\mathbb{Z})$$

είναι θετικώς ορισμένη, έχει διακρίνουσα 1 και $m = F_{\mathbf{A}}(0, 0, 1)$. Σύμφωνα με την πρόταση 5.7.42 αυτή είναι ισοδύναμη με την $(x_1, x_2, x_3) \longmapsto x_1^2 + x_2^2 + x_3^2$, οπότε ο m είναι παραστάσιμος ως άθροισμα των τετραγώνων τριών ακεραίων αριθμών. □

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

Ο G.L. Dirichlet[69] (1805-1859) απέδειξε το θεώρημα 5.7.44 με αναλυτικά μέσα, κάνοντας χρήση των λεγομένων *L-σειρών*. Διαφορετικές αποδείξεις οφείλονται στους H. Zassenhaus[70], A. Selberg[71], H.N. Shapiro[72] κ.ά.

[69] 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 A. και E. Ζαχαρίου, και επιμ. Γ. Λεγάτου, εκδόσεις Gutenberg, Αθήνα 1986, Κεφ. 7, σελ. 198-208.

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

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

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

5.7.45 Λήμμα. *Έστω $m \in \mathbb{N}$, $m \geq 2$. Εάν $m \equiv 2(\mathrm{mod}\, 4)$, τότε ο m είναι παραστάσιμος ως άθροισμα των τετραγώνων τριών ακεραίων αριθμών.*

ΑΠΟΔΕΙΞΗ. Επειδή $m \equiv 2(\mathrm{mod}\, 4) \Rightarrow$ μκδ$(4m, m-1) = 1$, υπάρχει (λόγω τού θεωρήματος 5.7.44) κάποιος πρώτος αριθμός p και κάποιος $j \in \mathbb{N}$, ούτως ώστε να ισχύει $p = 4mj + m - 1 = (4j+1)m - 1$. Προφανώς, $p \geq 5$. Θέτοντας $\kappa := 4j+1$ παρατηρούμε ότι

$$\left.\begin{array}{r} p = \kappa m - 1 \\ m \equiv 2(\mathrm{mod}\, 4) \Rightarrow \kappa m \equiv 2(\mathrm{mod}\, 4) \end{array}\right\} \Rightarrow p \equiv 1(\mathrm{mod}\, 4). \tag{5.120}$$

Αρκεί (λόγω τού πορίσματος 5.7.43) να δειχθεί ότι $\left(\frac{-\kappa}{p}\right) = 1$. Έστω $\kappa = q_1^{\nu_1} \cdots q_l^{\nu_l}$ ($l \in \mathbb{N}$) η παράσταση τού κ ως γινομένου κατάλληλων δυνάμεων $\nu_1, ..., \nu_l \in \mathbb{N}$ σαφώς διακεκριμένων πρώτων αριθμών $q_1, ..., q_l$. (Αυτοί οι πρώτοι είναι ≥ 3, διότι $\kappa \equiv 1(\mathrm{mod}\, 2)$.) Προφανώς,

$$p = \kappa m - 1 \equiv -1(\mathrm{mod}\, q_\varrho),\ \forall \varrho \in \{1, ..., l\}. \tag{5.121}$$

Επιπροσθέτως,

$$\kappa = \left(\prod_{\varrho \in \{1,...,l\}:\ q_\varrho \equiv 1(\mathrm{mod}\, 4)} q_\varrho^{\nu_\varrho} \right) \left(\prod_{\varrho \in \{1,...,l\}:\ q_\varrho \equiv 3(\mathrm{mod}\, 4)} q_\varrho^{\nu_\varrho} \right),$$

$[\kappa m \equiv 2(\mathrm{mod}\, 4)$ και $m \equiv 2(\mathrm{mod}\, 4)] \Rightarrow \kappa m \equiv m(\mathrm{mod}\, 4) \Rightarrow \kappa \equiv 1(\mathrm{mod}\, 4)$ (διότι $4 \nmid m$) και

$$1 \equiv \kappa \equiv \left(\prod_{\varrho \in \{1,...,l\}:\ q_\varrho \equiv 3(\mathrm{mod}\, 4)} (-1)^{\nu_\varrho} \right) (\mathrm{mod}\, 4),$$

οπότε

$$\left.\begin{array}{r} \displaystyle\prod_{\varrho \in \{1,...,l\}:\ q_\varrho \equiv 3(\mathrm{mod}\, 4)} (-1)^{\nu_\varrho} \in \{\pm 1\} \\ 4 \mid \displaystyle\prod_{\varrho \in \{1,...,l\}:\ q_\varrho \equiv 3(\mathrm{mod}\, 4)} (-1)^{\nu_\varrho} - 1 \end{array}\right\} \Rightarrow \prod_{\varrho \in \{1,...,l\}:\ q_\varrho \equiv 3(\mathrm{mod}\, 4)} (-1)^{\nu_\varrho} = 1. \tag{5.122}$$

Επομένως,

$$\left(\tfrac{-\kappa}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{\kappa}{p}\right) = \left(\tfrac{\kappa}{p}\right) = \prod_{\varrho=1}^{l} \left(\tfrac{q_\varrho}{p}\right)^{\nu_\varrho}$$

$$= \prod_{\varrho=1}^{l} \left(\tfrac{p}{q_\varrho}\right)^{\nu_\varrho} = \prod_{\varrho=1}^{l} \left(\tfrac{-1}{q_\varrho}\right)^{\nu_\varrho} = \prod_{\varrho \in \{1,...,l\}:\ q_\varrho \equiv 3(\mathrm{mod}\, 4)} (-1)^{\nu_\varrho} = 1,$$

όπου η πρώτη ισότητα προκύπτει από το 5.7.17 (iii), η δεύτερη από το ότι $\left(\frac{-1}{p}\right) = 1$ (βλ. (5.120) και (5.91)), η τρίτη από το (iii) τής προτάσεως 5.7.17, η τέταρτη από την (5.101), η πέμπτη από την (5.121) και το (i) τής προτάσεως 5.7.17, η έκτη από την (5.91) και η έβδομη από την (5.122). □

5.7.46 Λήμμα. *Έστω $m \in \mathbb{N}$. Εάν $m \equiv 1, 3$ ή $5 (\mathrm{mod}\, 8)$, τότε ο m είναι παραστάσιμος ως άθροισμα των τετραγώνων τριών ακεραίων αριθμών.*

ΑΠΟΔΕΙΞΗ. Επειδή $1 = 1^2 + 0^2 + 0^2$, μπορούμε να υποθέσουμε ότι $m \geq 2$. Θέτουμε

$$c := \begin{cases} 3, & \text{όταν} \quad m \equiv 1 (\mathrm{mod}\, 8), \\ 1, & \text{όταν} \quad m \equiv 3 (\mathrm{mod}\, 8), \\ 3, & \text{όταν} \quad m \equiv 5 (\mathrm{mod}\, 8). \end{cases}$$

Προφανώς,

$$\tfrac{cm-1}{2} \equiv \begin{cases} 1 (\mathrm{mod}\, 4), & \text{όταν} \quad m \equiv 1 (\mathrm{mod}\, 8), \\ 1 (\mathrm{mod}\, 4), & \text{όταν} \quad m \equiv 3 (\mathrm{mod}\, 8), \\ 3 (\mathrm{mod}\, 4), & \text{όταν} \quad m \equiv 5 (\mathrm{mod}\, 8). \end{cases}$$

Για κάθε $m \equiv 1, 3$ ή $5 (\mathrm{mod}\, 8)$ έχουμε $\frac{cm-1}{2} \equiv 1 (\mathrm{mod}\, 2)$, οπότε

$$\left.\begin{array}{l} \text{μκδ}(4m, \frac{cm-1}{2}) \mid m \\ \text{μκδ}(4m, \frac{cm-1}{2}) \mid cm - 1 \end{array}\right\} \Rightarrow \text{μκδ}(4m, \tfrac{cm-1}{2}) \mid 1 \Rightarrow \text{μκδ}(4m, \tfrac{cm-1}{2}) = 1.$$

Σύμφωνα με το θεώρημα 5.7.44 υπάρχει κάποιος πρώτος αριθμός $p > 2$ και κάποιος $j \in \mathbb{N}$, ούτως ώστε να ισχύει $p = 4mj + \frac{cm-1}{2}$. Θέτουμε $\kappa := 8j + c$. Προφανώς, $\kappa \equiv 1 (\mathrm{mod}\, 2)$. Επειδή $2p = (8j + c)m - 1 = \kappa m - 1$, αρκεί (λόγω τού πορίσματος 5.7.43) να δειχθεί ότι ο $-\kappa$ είναι τετραγωνικό ισοϋπόλοιπο κατά μόδιο $2p$.

Βήμα 1ο. Εάν ο $-\kappa$ είναι τετραγωνικό ισοϋπόλοιπο κατά μόδιο p, τότε ο $-\kappa$ είναι τετραγωνικό ισοϋπόλοιπο *και* κατά μόδιο $2p$. Πράγματι· εάν υποθέσουμε ότι υπάρχει κάποιος $x_0 \in \mathbb{Z}$ με $x_0^2 \equiv -\kappa (\mathrm{mod}\, p)$, τότε

$$(x_0 + p)^2 + \kappa \equiv x_0^2 + \kappa \equiv 0 (\mathrm{mod}\, p), \tag{5.123}$$

οπότε θέτοντας

$$x := \begin{cases} x_0, & \text{όταν} \quad x_0 \equiv 1 (\mathrm{mod}\, 2), \\ x_0 + p, & \text{όταν} \quad x_0 \equiv 0 (\mathrm{mod}\, 2), \end{cases}$$

λαμβάνουμε $2 \nmid x \Rightarrow x^2 + \kappa \equiv 0 (\mathrm{mod}\, 2) \underset{(5.123)}{\Longrightarrow} x^2 + \kappa \equiv 0 (\mathrm{mod}\, 2p)$, απ' όπου έπεται ότι $x^2 \equiv -\kappa (\mathrm{mod}\, 2p)$.

Βήμα 2ο. Βάσει των προαναφερθέντων στο 1ο βήμα αρκεί να αποδείξουμε ότι $\left(\frac{-\kappa}{p}\right) = 1$. Προς τούτο θεωρούμε την παράσταση $\kappa = q_1^{\nu_1} \cdots q_l^{\nu_l}$ ($l \in \mathbb{N}$) τού κ ως γινομένου κατάλληλων δυνάμεων $\nu_1, ..., \nu_l \in \mathbb{N}$ σαφώς διακεκριμένων πρώτων αριθμών $q_1, ..., q_l$. (Αυτοί οι πρώτοι είναι ≥ 3, διότι $\kappa \equiv 1 (\mathrm{mod}\, 2)$.) Επειδή ισχύει η ισότητα $2p = \kappa m - 1$, έχουμε

$$2p \equiv -1 (\mathrm{mod}\, \kappa) \Rightarrow 2p \equiv -1 (\mathrm{mod}\, q_\varrho) \text{ και } p \neq q_\varrho, \ \forall \varrho \in \{1, ..., l\}. \tag{5.124}$$

Περίπτωση πρώτη. Εάν $m \equiv 1$ ή $3 (\mathrm{mod}\, 8)$, τότε $p \equiv 1 (\mathrm{mod}\, 4)$ και

$$\left(\frac{-\kappa}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{\kappa}{p}\right) = \left(\frac{\kappa}{p}\right) = \prod_{\varrho=1}^{l} \left(\frac{q_\varrho}{p}\right)^{\nu_\varrho} = \prod_{\varrho=1}^{l} \left(\frac{p}{q_\varrho}\right)^{\nu_\varrho}, \tag{5.125}$$

όπου η πρώτη και η τρίτη ισότητα προκύπτουν από το (iii) τής προτάσεως 5.7.17, η δεύτερη από την (5.91) και η τέταρτη από την (5.101).

Περίπτωση δεύτερη. Εάν $m \equiv 5 (\mathrm{mod}\, 8)$, τότε $p \equiv 3 (\mathrm{mod}\, 4)$ και $\kappa \equiv 3 (\mathrm{mod}\, 8)$. Επειδή

$$\kappa = \left(\prod_{\varrho \in \{1,\ldots,l\}:\ q_\varrho \equiv 1 (\mathrm{mod}\, 4)} q_\varrho^{\nu_\varrho} \right) \left(\prod_{\varrho \in \{1,\ldots,l\}:\ q_\varrho \equiv 3 (\mathrm{mod}\, 4)} q_\varrho^{\nu_\varrho} \right)$$

και $\kappa \equiv 3 (\mathrm{mod}\, 8) \Rightarrow \kappa \equiv -1 (\mathrm{mod}\, 4)$, έχουμε

$$-1 \equiv \kappa \equiv \left(\prod_{\varrho \in \{1,\ldots,l\}:\ q_\varrho \equiv 3 (\mathrm{mod}\, 4)} (-1)^{\nu_\varrho} \right) (\mathrm{mod}\, 4),$$

οπότε

$$\left.\begin{array}{l} \displaystyle\prod_{\varrho \in \{1,\ldots,l\}:\ q_\varrho \equiv 3 (\mathrm{mod}\, 4)} (-1)^{\nu_\varrho} \in \{\pm 1\} \\ 4 \mid \displaystyle\prod_{\varrho \in \{1,\ldots,l\}:\ q_\varrho \equiv 3 (\mathrm{mod}\, 4)} (-1)^{\nu_\varrho} + 1 \end{array}\right\} \Rightarrow \prod_{\varrho \in \{1,\ldots,l\}:\ q_\varrho \equiv 3 (\mathrm{mod}\, 4)} (-1)^{\nu_\varrho} = -1. \tag{5.126}$$

Επομένως,

$$\begin{aligned} \left(\frac{-\kappa}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{\kappa}{p}\right) = -\left(\frac{\kappa}{p}\right) = -\prod_{\varrho=1}^{l} \left(\frac{q_\varrho}{p}\right)^{\nu_\varrho} \\ &= -\left(\prod_{\varrho \in \{1,\ldots,l\}:\ q_\varrho \equiv 1 (\mathrm{mod}\, 4)} \left(\frac{q_\varrho}{p}\right)^{\nu_\varrho} \right) \left(\prod_{\varrho \in \{1,\ldots,l\}:\ q_\varrho \equiv 3 (\mathrm{mod}\, 4)} \left(\frac{q_\varrho}{p}\right)^{\nu_\varrho} \right) \\ &= -\left(\prod_{\varrho:\ q_\varrho \equiv 1 (\mathrm{mod}\, 4)} \left(\frac{p}{q_\varrho}\right)^{\nu_\varrho} \right) \left(\prod_{\varrho:\ q_\varrho \equiv 3 (\mathrm{mod}\, 4)} \left(\frac{p}{q_\varrho}\right)^{\nu_\varrho} \right) \left(\prod_{\varrho:\ q_\varrho \equiv 3 (\mathrm{mod}\, 4)} (-1)^{\nu_\varrho} \right), \end{aligned}$$

όπου η πρώτη και η τρίτη ισότητα προκύπτουν από το (iii) τής προτάσεως 5.7.17, η δεύτερη από την (5.91) και η πέμπτη από την (5.101), οπότε η (5.126) δίδει τελικώς

$$\left(\frac{-\kappa}{p}\right) = \prod_{\varrho=1}^{l} \left(\frac{p}{q_\varrho}\right)^{\nu_\varrho}. \tag{5.127}$$

Διευκολυντική έκφραση τού $\left(\frac{-\kappa}{p}\right)$ σε αμφότερες τις περιπτώσεις. Λόγω των (5.125)

και (5.127) έχουμε *για κάθε* $m \equiv 1,3$ ή $5 (\mathrm{mod}\, 8)$

$$\begin{aligned}
\left(\tfrac{-\kappa}{p}\right) &= \prod_{\varrho=1}^{l} \left(\tfrac{p}{q_\varrho}\right)^{\nu_\varrho} = \prod_{\varrho=1}^{l} \left(\tfrac{2^2}{q_\varrho}\right)^{\nu_\varrho} \left(\tfrac{p}{q_\varrho}\right)^{\nu_\varrho} \\
&= \prod_{\varrho=1}^{l} \left(\tfrac{2}{q_\varrho}\right)^{\nu_\varrho} \prod_{\varrho=1}^{l} \left(\tfrac{2p}{q_\varrho}\right)^{\nu_\varrho} = \prod_{\varrho=1}^{l} \left(\tfrac{2}{q_\varrho}\right)^{\nu_\varrho} \prod_{\varrho=1}^{l} \left(\tfrac{-1}{q_\varrho}\right)^{\nu_\varrho} \\
&= \left(\prod_{\varrho\in\{1,\ldots,l\}:\ q_\varrho\equiv 3 \text{ ή } 5 (\mathrm{mod}\, 8)} (-1)^{\nu_\varrho} \right) \left(\prod_{\varrho\in\{1,\ldots,l\}:\ q_\varrho\equiv 3 \text{ ή } 7 (\mathrm{mod}\, 8)} (-1)^{\nu_\varrho} \right) \\
&= \prod_{\varrho\in\{1,\ldots,l\}:\ q_\varrho\equiv 5 \text{ ή } 7 (\mathrm{mod}\, 8)} (-1)^{\nu_\varrho},
\end{aligned}$$

όπου η δεύτερη και η τρίτη ισότητα έπονται από τα (ii) και (iii) τής 5.7.17, η τέταρτη από την (5.124) και το (i) τής προτάσεως 5.7.17, η πέμπτη από τις (5.92) και[73] (5.91), και η έκτη από το ότι οι παράγοντες που αντιστοιχούν στους δείκτες ϱ με $q_\varrho \equiv 3 (\mathrm{mod}\, 8)$ μπορούν να απαλειφθούν (αφού εμφανίζονται υψωμένοι στο τετράγωνο).

Βήμα 3ο. Εκμεταλλευόμενοι την έκφραση τού $\left(\frac{-\kappa}{p}\right)$ (την προκύψασα στο τέλος τού 2ου βήματος) αρκεί να αποδείξουμε ότι για κάθε $m \equiv 1,3$ ή $5 (\mathrm{mod}\, 8)$ ισχύει η ισοτιμία

$$\sum_{\varrho\in\{1,\ldots,l\}:\ q_\varrho\equiv 5 \text{ ή } 7 (\mathrm{mod}\, 8)} \nu_\varrho \equiv 0 (\mathrm{mod}\, 2). \tag{5.128}$$

Εν πρώτοις παρατηρούμε ότι

$$\begin{aligned}
\kappa &= \underbrace{\prod_{\varrho:\ q_\varrho\equiv 1 (\mathrm{mod}\, 8)} q_\varrho^{\nu_\varrho}}_{\equiv 1 (\mathrm{mod}\, 8)} \prod_{\varrho:\ q_\varrho\equiv 3 (\mathrm{mod}\, 8)} q_\varrho^{\nu_\varrho} \prod_{\varrho:\ q_\varrho\equiv 5 (\mathrm{mod}\, 8)} q_\varrho^{\nu_\varrho} \prod_{\varrho:\ q_\varrho\equiv 7 (\mathrm{mod}\, 8)} q_\varrho^{\nu_\varrho} \\
&\equiv \left(\prod_{\varrho:\ q_\varrho\equiv 3 (\mathrm{mod}\, 8)} 3^{\nu_\varrho} \prod_{\varrho:\ q_\varrho\equiv 5 (\mathrm{mod}\, 8)} (-3)^{\nu_\varrho} \prod_{\varrho:\ q_\varrho\equiv 7 (\mathrm{mod}\, 8)} (-1)^{\nu_\varrho} \right) (\mathrm{mod}\, 8) \\
&\equiv \left(\prod_{\varrho:\ q_\varrho\equiv 3 \text{ ή } 5 (\mathrm{mod}\, 8)} 3^{\nu_\varrho} \prod_{\varrho:\ q_\varrho\equiv 5 \text{ ή } 7 (\mathrm{mod}\, 8)} (-1)^{\nu_\varrho} \right) (\mathrm{mod}\, 8) \\
&\equiv \left(3^{\sum_{\varrho:\ q_\varrho\equiv 3 \text{ ή } 5 (\mathrm{mod}\, 8)} \nu_\varrho} \right) \left((-1)^{\sum_{\varrho:\ q_\varrho\equiv 5 \text{ ή } 7 (\mathrm{mod}\, 8)} \nu_\varrho} \right) (\mathrm{mod}\, 8).
\end{aligned}$$

• Εάν $m \equiv 1$ ή $5 (\mathrm{mod}\, 8)$, τότε $c = 3 \Rightarrow \kappa = 8j+3 \equiv 3 (\mathrm{mod}\, 8)$, οπότε κατ' ανάγκην

$$\sum_{\varrho:\ q_\varrho\equiv 3 \text{ ή } 5 (\mathrm{mod}\, 8)} \nu_\varrho \equiv 1 (\mathrm{mod}\, 2) \quad \text{και} \quad \sum_{\varrho:\ q_\varrho\equiv 5 \text{ ή } 7 (\mathrm{mod}\, 8)} \nu_\varrho \equiv 0 (\mathrm{mod}\, 2),$$

και η (5.128) είναι αληθής.

[73] Σημειωτέον ότι $q_\varrho \equiv 3 (\mathrm{mod}\, 4) \Leftrightarrow q_\varrho \equiv 3$ ή $7 (\mathrm{mod}\, 8)$.

• Εάν $m \equiv 3(\mathrm{mod}\,8)$, τότε $c = 1 \Rightarrow \kappa = 8j+1 \equiv 1\,(\mathrm{mod}\,8)$, οπότε κατ' ανάγκην

$$\sum_{\varrho:\ q_\varrho \equiv 3 \text{ ή } 5(\mathrm{mod}\,8)} \nu_\varrho \equiv 0\,(\mathrm{mod}\,2) \quad \text{και} \quad \sum_{\varrho:\ q_\varrho \equiv 5 \text{ ή } 7(\mathrm{mod}\,8)} \nu_\varrho \equiv 0(\mathrm{mod}\,2),$$

και η (5.128) είναι *και* σε αυτήν την περίπτωση αληθής. □

5.7.47 Λήμμα. *Για κάθε $a \in \mathbb{Z}$ έχουμε $a^2 \equiv 0, 1$ ή $4(\mathrm{mod}\,8)$.*

ΑΠΟΔΕΙΞΗ. Επειδή $a = 8q + r$ για κάποιον $q \in \mathbb{Z}$ και $r \in \{0, 1, ..., 7\}$, και το τετράγωνό του ισούται με $a^2 = 8(8q^2 + 2qr) + r^2 \equiv r^2(\mathrm{mod}\,8)$. Το τελευταίο, υπολογιζόμενο $\mathrm{mod}\,8$, δίδει

r	0	1	2	3	4	5	6	7
$r^2 \equiv ...\,(\mathrm{mod}\,8)$	0	1	4	1	0	1	4	1

οπότε ο ισχυρισμός είναι αληθής. □

5.7.48 Λήμμα. *Για έναν $m \in \mathbb{N}$ οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Ο m ισούται με το άθροισμα των τετραγώνων τριών ακεραίων αριθμών.*

(ii) *Ο $4m$ ισούται με το άθροισμα των τετραγώνων τριών ακεραίων αριθμών.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $m = x_1^2 + x_2^2 + x_3^2$ για κάποιους $x_1, x_2, x_3 \in \mathbb{Z}$, τότε

$$4m = (2x_1)^2 + (2x_2)^2 + (2x_3)^2.$$

(ii)⇒(i) Εάν $4m = x_1^2 + x_2^2 + x_3^2$ για κάποιους $x_1, x_2, x_3 \in \mathbb{Z}$, τότε $x_j^2 \equiv 0, 1$ ή $4(\mathrm{mod}\,8)$ για κάθε $j \in \{1, 2, 3\}$. (Βλ. λήμμα 5.7.47.) Επειδή $4m \equiv 0$ ή $4(\mathrm{mod}\,8)$, έχουμε κατ' ανάγκην $x_j^2 \not\equiv 1(\mathrm{mod}\,8)$ και $x_j \equiv 0(\mathrm{mod}\,2)$ για κάθε $j \in \{1, 2, 3\}$. Επομένως, $m = \sum_{j=1}^{3} (\frac{1}{2}x_j)^2$. □

5.7.49 Θεώρημα. (Πότε είναι ένας $n \in \mathbb{N}$ άθροισμα τριών τετραγώνων;) *Για έναν $n \in \mathbb{N}$ οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Ο n ισούται με το άθροισμα των τετραγώνων τριών ακεραίων αριθμών.*

(ii) *Ο n δεν γράφεται υπό τη μορφή $n = 4^\nu(8\xi + 7)$ για κάποιους $\nu, \xi \in \mathbb{N}_0$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Ας υποθέσουμε ότι $n = 4^\nu(8\xi + 7)$ για κάποιους $\nu, \xi \in \mathbb{N}_0$ και ότι ο n γράφεται ως άθροισμα των τετραγώνων τριών ακεραίων αριθμών. Εάν $\nu \geq 1$, τότε εφαρμόζουμε ν φορές τη συνεπαγωγή (ii)⇒(i) τού λήμματος 5.7.48. Έτσι, για κάθε $\nu \geq 0$ συμπεραίνουμε ότι ο $8\xi+7$ γράφεται ως άθροισμα $x_1^2+x_2^2+x_3^2$ για κάποιους $x_1, x_2, x_3 \in \mathbb{Z}$. Επειδή (σύμφωνα με το λήμμα 5.7.47) $x_j^2 \equiv 0, 1$ ή $4(\mathrm{mod}\,8)$ για κάθε $j \in \{1, 2, 3\}$, λαμβάνουμε $x_1^2+x_2^2+x_3^2 \equiv 0, 1, 2, 3, 4, 5$ ή $6(\mathrm{mod}\,8)$. Όμως $8\xi + 7 \equiv 7(\mathrm{mod}\,8)$. Άτοπο!

(ii)⇒(i) Ας υποθέσουμε ότι ο n δεν γράφεται υπό τη μορφή $n = 4^\nu(8\xi + 7)$ για κάποιους $\nu, \xi \in \mathbb{N}_0$. Τότε ο n γράφεται υπό τη μορφή $n = 4^\nu m$ για κάποιους $\nu \in \mathbb{N}_0$

και $m \in \mathbb{N}$ με $4 \nmid m$ και $m \not\equiv 7 (\mathrm{mod}\, 8)$. Εάν ο m είναι άρτιος, τότε $m \equiv 2 (\mathrm{mod}\, 4)$ και βάσει τού λήμματος 5.7.45 είναι παραστάσιμος ως άθροισμα των τετραγώνων τριών ακεραίων αριθμών. Εάν ο m είναι περιττός, τότε $m \equiv 1, 3$ ή $5 (\mathrm{mod}\, 8)$ και είναι (και σε αυτήν την περίπτωση) παραστάσιμος ως άθροισμα των τετραγώνων τριών ακεραίων αριθμών επί τη βάσει τού λήμματος 5.7.46. Άρα *και ο ίδιος* ο n είναι παραστάσιμος ως άθροισμα των τετραγώνων τριών ακεραίων αριθμών. (Αρκεί να εφαρμοσθεί η συνεπαγωγή (i)⇒(ii) τού λήμματος 5.7.48 ν φορές όταν $\nu \geq 1$.) □

5.7.50 Παρατήρηση. (i) Ένας φυσικός αριθμός ενδέχεται να γράφεται ως άθροισμα τριών τετραγώνων κατά διαφορετικούς τρόπους. Επί παραδείγματι,

$$182 = 1^2 + 9^2 + 10^2 = 5^2 + 6^2 + 11^2.$$

(ii) Οι φυσικοί αριθμοί $n \leq 100$ που *δεν γράφονται* ως άθροισμα τριών τετραγώνων είναι οι

$$7, 15, 23, 28, 31, 39, 47, 55, 60, 63, 71, 79, 87, 92, 95.$$

► **Αθροίσματα τεσσάρων τετραγώνων**. Η παρούσα ενότητα θα κλείσει με την παράθεση μιας *σύντομης* αποδείξεως τού *θεωρήματος* 5.7.53 *των τεσσάρων τετραγώνων* (τού Lagrange) που οφείλεται στους M. Newman[74] και C. Small[75], και στηρίζεται σε πολύ απλές ιδιότητες τού δακτυλίου $\mathrm{Mat}_{2\times 2}(\mathbb{Z}[i])$.

5.7.51 Λήμμα. *Εάν m είναι είτε ένας πρώτος αριθμός p είτε το γινόμενο $p_1 \cdots p_k$ σαφώς διακεκριμένων πρώτων αριθμών $p_1, ..., p_k$, όπου $k \geq 2$, τότε κάθε στοιχείο τού δακτυλίου $\mathbb{Z}_m$ ισούται με το άθροισμα των τετραγώνων δύο στοιχείων τού $\mathbb{Z}_m$.*

ΑΠΟΔΕΙΞΗ. Όταν $m = p$, όπου p πρώτος, τούτο είναι γνωστό. (Βλ. άσκηση **1**-**12**.) Όταν $m = p_1 \cdots p_k$, όπου $k \geq 2$, η απεικόνιση

$$f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k},\ [a]_m \longmapsto f([a]_m) := ([a]_{p_1}, ..., [a]_{p_k}),\ \forall a \in \mathbb{Z},$$

αποτελεί *ισομορφισμό* δακτυλίων. (Βλ. πόρισμα 3.4.9 και εδάφιο 3.3.4 (i).) Επομένως, για κάθε $a \in \mathbb{Z}$ η κλάση ισοτιμίας $[a]_m \in \mathbb{Z}_m$ είναι η εικόνα $f^{-1}(([b_1]_{p_1}, ..., [b_k]_{p_k}))$ μίας (και μόνον) k-άδας κλάσεων $([b_1]_{p_1}, ..., [b_k]_{p_k})$ μέσω τού αντιστρόφου του f^{-1} για κατάλληλους $b_1, ..., b_k \in \mathbb{Z}$. Επειδή για κάθε $j \in \{1, ..., k\}$ η κλάση $[b_j]_{p_j}$ γράφεται ως άθροισμα τετραγώνων $[b_j]_{p_j} = [c_j]^2_{p_j} + [d_j]^2_{p_j}$ για κά-

[74] M. Newman: *Integral Matrices*, Academic Press, 1972. (Βλ. Κεφ. XI, 14, σελ. 215.)

[75] C. Small: *A simple proof of the four-squares theorem*, The American Mathematical Monthly **89** (1982), 59-61.

ποιους $c_j, d_j \in \mathbb{Z}$, έχουμε

$$\begin{aligned}
[a]_m &= f^{-1}(([b_1]_{p_1}, ..., [b_k]_{p_k})) = f^{-1}(([c_1]_{p_1}^2 + [d_1]_{p_1}^2, ..., [c_k]_{p_k}^2 + [d_k]_{p_k}^2)) \\
&= f^{-1}(([c_1]_{p_1}^2, ..., [c_k]_{p_k}^2) + ([d_1]_{p_1}^2, ..., [d_k]_{p_k}^2)) \\
&= f^{-1}(([c_1]_{p_1}, ..., [c_k]_{p_k})^2 + ([d_1]_{p_1}, ..., [d_k]_{p_k})^2) \\
&= f^{-1}(([c_1]_{p_1}, ..., [c_k]_{p_k})^2) + f^{-1}(([d_1]_{p_1}, ..., [d_k]_{p_k})^2) \\
&= (f^{-1}(([c_1]_{p_1}, ..., [c_k]_{p_k})))^2 + (f^{-1}(([d_1]_{p_1}, ..., [d_k]_{p_k})))^2,
\end{aligned}$$

οπότε *και* η κλάση $[a]_m \in \mathbb{Z}_m$ ισούται με το άθροισμα των τετραγώνων δύο στοιχείων τού $\mathbb{Z}_m$. □

5.7.52 Λήμμα. *Έστω ότι* $m, n, c, d \in \mathbb{Z}$ *με* $n \geq 1$ *και*

$$\mathbf{A} := \begin{pmatrix} n & c+di \\ c-di & m \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[i]).$$

Εάν $\det(\mathbf{A}) = 1$, *τότε*[76] $\exists \mathbf{B} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[i])$: $\mathbf{A} = \mathbf{B}\mathbf{B}^*$.

ΑΠΟΔΕΙΞΗ. Επειδή $mn = c^2 + d^2 + 1 \geq 1$ και $n \geq 1$, έχουμε $m \geq 1$. Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς το άθροισμα $c^2 + d^2$. Εάν $c^2 + d^2 = 0$, τότε $c = d = 0$ και $\mathbf{A} = \mathbf{I}_2$, οπότε αρκεί να θέσουμε $\mathbf{B} := \mathbf{I}_2$. Ας υποθέσουμε εφεξής ότι $c^2 + d^2 \geq 1$ και ότι ο ισχυρισμός είναι αληθής για πίνακες έχοντες το αντίστοιχο άθροισμα των τετραγώνων $< c^2 + d^2$.

Περίπτωση πρώτη. Εάν $1 \leq n \leq m$, τότε

$$\text{είτε} \quad |c| > \tfrac{n}{2} \quad \text{είτε} \quad |d| > \tfrac{n}{2}. \tag{5.129}$$

Πράγματι· για $n = 1$ τούτο είναι προφανές (διότι τουλάχιστον ένας εκ των c, d είναι $\neq 0$), ενώ για $n \geq 2$ η ταυτόχρονη ισχύς των ανισοϊσοτήτων $|c| \leq \frac{n}{2}$ και $|d| \leq \frac{n}{2}$ θα οδηγούσε σε άτοπο, καθόσον θα είχαμε

$$n^2 \leq nm = c^2 + d^2 + 1 \leq \left(\tfrac{n}{2}\right)^2 + \left(\tfrac{n}{2}\right)^2 + 1 = \tfrac{n^2}{2} + 1 < n^2.$$

Θέτοντας $\mathbf{A}' := \mathbf{C}\mathbf{A}\mathbf{C}^*$, όπου

$$\mathbf{C} := \begin{pmatrix} 1 & 0 \\ x - yi & 1 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[i]),$$

με τους x, y (κάτωθι προσδιοριστέους) ακεραίους, λαμβάνουμε

$$\mathbf{A}' = \begin{pmatrix} n & c'+d'i \\ c'-d'i & nx^2 + ny^2 + 2cx + 2dy + m \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[i]),$$

όπου $c' := nx + c$ και $d' := ny + d$. Μάλιστα, επειδή $\det(\mathbf{C}) = \det(\mathbf{C}^*) = 1$, έχουμε

$$\det(\mathbf{A}') = \det(\mathbf{C}\mathbf{A}\mathbf{C}^*) = \det(\mathbf{C})\det(\mathbf{A})\det(\mathbf{C}^*) = \det(\mathbf{A}) = 1.$$

[76] Ως $\mathbf{B}^*$ συμβολίζεται ο *αναστροφοσυζυγής* τού $\mathbf{B}$.

Για να είμαστε, λοιπόν, σε θέση να εφαρμόσουμε την επαγωγική μας υπόθεση, αρκεί να επιλέξουμε *κατάλληλους ακεραίους* x, y, ούτως ώστε να ισχύει η ανισότητα $c'^2 + d'^2 < c^2 + d^2$. Λαμβάνοντας υπ' όψιν τη συνθήκη (5.129), η επιλογή των x, y γίνεται ως ακολούθως:

(i) Εάν $c > \frac{n}{2}$, τότε για $x = -1$ και $y = 0$ έχουμε $c' = c - n < c$ και

$$c'^2 + d'^2 = (c-n)^2 + d^2 < c^2 + d^2.$$

(ii) Εάν $c < -\frac{n}{2}$, τότε για $x = 1$ και $y = 0$ έχουμε $c' = c + n < \frac{n}{2} < -c$ και

$$c'^2 + d'^2 = (c+n)^2 + d^2 < c^2 + d^2.$$

(iii) Εάν $d > \frac{n}{2}$, τότε για $x = 0$ και $y = -1$ έχουμε $d' = d - n < d$ και

$$c'^2 + d'^2 = c^2 + (d-n)^2 < c^2 + d^2.$$

(iv) Εάν $d < -\frac{n}{2}$, τότε για $x = 0$ και $y = 1$ έχουμε $d' = d + n < \frac{n}{2} < -d$ και

$$c'^2 + d'^2 = c^2 + (d+n)^2 < c^2 + d^2.$$

Για τα ανωτέρω (συγκεκριμένα) x και y υπάρχει (σύμφωνα με την επαγωγική μας υπόθεση) πίνακας $\mathbf{D} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[i])$: $\mathbf{A}' = \mathbf{D}\mathbf{D}^*$, οπότε θέτοντας $\mathbf{B} := \mathbf{C}^{-1}\mathbf{D}$ λαμβάνουμε

$$\mathbf{A} = \mathbf{C}^{-1}\mathbf{A}'\,(\mathbf{C}^*)^{-1} = \mathbf{C}^{-1}\mathbf{D}\mathbf{D}^*\,(\mathbf{C}^*)^{-1} = (\mathbf{C}^{-1}\mathbf{D})(\mathbf{C}^{-1}\mathbf{D})^* = \mathbf{B}\mathbf{B}^*. \quad (5.130)$$

Περίπτωση δεύτερη. Εάν $1 \le m \le n$, τότε ισχύει (κατ' αναλογίαν)

$$\text{είτε} \quad |c| > \tfrac{m}{2} \quad \text{είτε} \quad |d| > \tfrac{m}{2}. \quad (5.131)$$

Πράγματι· για $m = 1$ τούτο είναι προφανές (διότι τουλάχιστον ένας εκ των c, d είναι $\neq 0$), ενώ για $m \ge 2$ η ταυτόχρονη ισχύς των ανισοϊσοτήτων $|c| \le \frac{m}{2}$ και $|d| \le \frac{m}{2}$ θα οδηγούσε σε άτοπο, καθόσον θα είχαμε

$$m^2 \le nm = c^2 + d^2 + 1 \le \left(\tfrac{m}{2}\right)^2 + \left(\tfrac{m}{2}\right)^2 + 1 = \tfrac{m^2}{2} + 1 < m^2.$$

Θέτοντας $\mathbf{A}' := \mathbf{C}\mathbf{A}\mathbf{C}^*$, όπου

$$\mathbf{C} := \begin{pmatrix} 1 & x+yi \\ 0 & 1 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[i]),$$

με τους x, y (κάτωθι προσδιοριστέους) ακεραίους, λαμβάνουμε

$$\mathbf{A}' = \begin{pmatrix} n + 2cx + 2dy + mx^2 + my^2 & c' + d'i \\ c' - d'i & m \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[i]),$$

όπου $c' := mx + c$ και $d' := my + d$. Μάλιστα, επειδή $\det(\mathbf{C}) = \det(\mathbf{C}^*) = 1$, έχουμε $\det(\mathbf{A}') = \det(\mathbf{C}\mathbf{A}\mathbf{C}^*) = \det(\mathbf{C})\det(\mathbf{A})\det(\mathbf{C}^*) = \det(\mathbf{A}) = 1$. Για να

είμαστε, λοιπόν, σε θέση να εφαρμόσουμε την επαγωγική μας υπόθεση, αρκεί να επιλέξουμε *κατάλληλους* x, y, ούτως ώστε να ισχύει η ανισότητα $c'^2 + d'^2 < c^2 + d^2$. Λαμβάνοντας υπ' όψιν τη συνθήκη (5.131), η επιλογή των x, y γίνεται ως ακολούθως:

(i) Εάν $c > \frac{m}{2}$, τότε για $x = -1$ και $y = 0$ έχουμε $c' = c - m < c$ και

$$c'^2 + d'^2 = (c-m)^2 + d^2 < c^2 + d^2.$$

(ii) Εάν $c < -\frac{m}{2}$, τότε για $x = 1$ και $y = 0$ έχουμε $c' = c + m < \frac{m}{2} < -c$ και

$$c'^2 + d'^2 = (c+m)^2 + d^2 < c^2 + d^2.$$

(iii) Εάν $d > \frac{m}{2}$, τότε για $x = 0$ και $y = -1$ έχουμε $d' = d - m < d$ και

$$c'^2 + d'^2 = c^2 + (d-m)^2 < c^2 + d^2.$$

(iv) Εάν $d < -\frac{m}{2}$, τότε για $x = 0$ και $y = 1$ έχουμε $d' = d + m < \frac{m}{2} < -d$ και

$$c'^2 + d'^2 = c^2 + (d+m)^2 < c^2 + d^2.$$

Για τα ανωτέρω (συγκεκριμένα) x και y υπάρχει (σύμφωνα με την επαγωγική μας υπόθεση) πίνακας $\mathbf{D} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[i])$: $\mathbf{A}' = \mathbf{D}\mathbf{D}^*$, οπότε θέτοντας $\mathbf{B} := \mathbf{C}^{-1}\mathbf{D}$ λαμβάνουμε εκ νέου την ισότητα (5.130). □

5.7.53 Θεώρημα. («Θεώρημα των τεσσάρων τετραγώνων», Lagrange, 1770.**)** *Κάθε $n \in \mathbb{N}$ μπορεί να παρασταθεί ως άθροισμα*

$$\boxed{n = w^2 + x^2 + y^2 + z^2}$$

των τετραγώνων τεσσάρων ακεραίων αριθμών w, x, y και z.

ΑΠΟΔΕΙΞΗ. Έστω $n \in \mathbb{N}$. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι ο n δεν διαιρείται διά τού τετραγώνου ενός ακεραίου a με $|a| \geq 2$, διότι εάν $n = a^2 n'$ και $n' = w^2 + x^2 + y^2 + z^2$ για κάποιους ακεραίους αριθμούς w, x, y και z, τότε

$$n = (aw)^2 + (ax)^2 + (ay)^2 + (az)^2.$$

Το λήμμα 5.7.51 εγγυάται την ύπαρξη ακεραίων αριθμών c, d, τέτοιων ώστε να ισχύει η ισότητα $[-1]_n = [c]_n^2 + [d]_n^2$. Επομένως,

$$\exists m \in \mathbb{Z} : mn - \left(c^2 + d^2\right) = 1,$$

απ' όπου έπεται ότι η ορίζουσα τού πίνακα

$$\mathbf{A} := \begin{pmatrix} n & c+di \\ c-di & m \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[i])$$

ισούται με 1. Κατά το λήμμα 5.7.52,

$$\exists\, \mathbf{B} = \begin{pmatrix} w+xi & y+zi \\ w'+x'i & y'+z'i \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[i]) : \mathbf{A} = \mathbf{B}\mathbf{B}^*.$$

Θέτοντας $u := ww' + xx' + yy' + zz' + i(xw' - wx' + zy' - yz')$, αυτό σημαίνει ότι

$$\begin{pmatrix} n & c+di \\ c-di & m \end{pmatrix} = \begin{pmatrix} w+xi & y+zi \\ w'+x'i & y'+z'i \end{pmatrix} \begin{pmatrix} w-xi & w'-x'i \\ y-zi & y'-z'i \end{pmatrix}$$

$$= \begin{pmatrix} w^2+x^2+y^2+z^2 & u \\ \overline{u} & (w')^2+(x')^2+(y')^2+(z')^2 \end{pmatrix}$$

και, ιδιαιτέρως, ότι $n = w^2 + x^2 + y^2 + z^2$. □

5.7.54 Σημείωση. (i) Η ανωτέρω απόδειξη τού θεωρήματος 5.7.53 είναι *ανεξάρτητη* τής (μακροσκελούς) αποδείξεως τού θεωρήματος 5.7.49. Βεβαίως, το θεώρημα 5.7.53 μπορεί να ιδωθεί και ως *άμεσο πόρισμα* τού θεωρήματος 5.7.49: Εάν ένας $n \in \mathbb{N}$ είναι παραστάσιμος ως άθροισμα των τετραγώνων *τριών* ακεραίων αριθμών, τότε είναι παραστάσιμος και ως άθροισμα *τεσσάρων* τετραγώνων. (Αρκεί κανείς να προσθέσει το 0^2 στο άθροισμα.) Στην περίπτωση που ο θεωρούμενος $n \in \mathbb{N}$ *δεν είναι* παραστάσιμος ως άθροισμα των τετραγώνων *τριών* ακεραίων αριθμών, έχουμε $n = 4^\nu(8\xi + 7)$ για κάποιους $\nu, \xi \in \mathbb{N}_0$. Εν τοιαύτη περιπτώσει, το θεώρημα 5.7.49 μας πληροφορεί ότι

$$\exists\ (x, y, z) \in \mathbb{Z}^3 : 8\xi + 6 = x^2 + y^2 + z^2,$$

οπότε $8\xi + 7 = 1^2 + x^2 + y^2 + z^2$ και $n = (2^\nu)^2 + (2^\nu x)^2 + (2^\nu y)^2 + (2^\nu z)^2$.

(ii) Ένας φυσικός αριθμός ενδέχεται να γράφεται ως άθροισμα τεσσάρων τετραγώνων κατά διαφορετικούς τρόπους. Επί παραδείγματι,

$$\begin{aligned} 36 &= 6^2 + 0^2 + 0^2 + 0^2 = 4^2 + 4^2 + 2^2 + 0^2 \\ &= 3^2 + 3^2 + 3^2 + 3^2 = 5^2 + 3^2 + 1^2 + 1^2. \end{aligned}$$

Από την άλλη μεριά, υπάρχει μια (άπειρη) ακολουθία φυσικών αριθμών που γράφονται ως άθροισμα τεσσάρων τετραγώνων κατά έναν και μόνον τρόπο (μέχρις αναδιατάξεως των τεσσάρων προσθετέων):

$$1, 2, 3, 5, 6, 7, 8, 11, 14, 15, 23, 24, 32, 56, 96, 128, 224, 384,$$
$$512, 896, 1536, 2048, 3584, 6144, 8192, 14336, 24576, 32768, \ldots.$$

(iii) Το 1834 ο Carl Gustav Jacob Jacobi (1804-1851) απέδειξε ότι το πλήθος όλων των δυνατών παραστάσεων ενός $n \in \mathbb{N}$ ως αθροίσματος τεσσάρων τετραγώνων ισούται με[77]

$$8 \sum_{\{d\in\mathbb{N}:\ d|n \text{ και } 4\nmid d\}} d.$$

[77] Βλ. M.D. Hirschhorn: *A simple proof of Jacobis four-square theorem*, Proc. Amer. Math. Soc. **101** (1987), 436-438.

5.8 ΑΡΙΘΜΟΘΕΩΡΗΤΙΚΕΣ ΕΦΑΡΜΟΓΕΣ ΙΙ: ΕΙΔΙΚΕΣ ΔΙΟΦΑΝΤΙΚΕΣ ΕΞΙΣΩΣΕΙΣ

Η εργασία με περιοχές μονοσήμαντης παραγοντοποιήσεως καθίσταται εποικοδομητική ακόμη και κατά την επίλυση ορισμένων διοφαντικών εξισώσεων. Στην παρούσα ενότητα δίδονται δύο παραδείγματα: Η *εξίσωση τού Mordell* (για *ειδικές τιμές* τής παραμέτρου της) και η *εξίσωση των Ramanujan και Nagell*.

► **Εξίσωση τού Mordell.** Εντός τού $\mathbb{R}^2$ αυτή περιγράφει κάποια ειδική ελλειπτική καμπύλη. Ζητείται ο εντοπισμός των κιγκλιδωματικών σημείων (ήτοι των σημείων τού $\mathbb{R}^2$ των εχόντων αμφότερες τις συντεταγμένες τους ακέραιες) που κείνται επί τής καμπύλης.

5.8.1 Ορισμός. Η διοφαντική εξίσωση

$$\boxed{y^2 = x^3 + k,} \tag{5.132}$$

όπου $k \in \mathbb{Z}\setminus\{0\}$, καλείται **εξίσωση τού Mordell**[78]**,** έχουσα ως παράμετρό της τον k. Είναι γνωστό[79] ότι το σύνολο των ακεραίων λύσεων τής (5.132) είναι είτε *πεπερασμένο* είτε το $\varnothing$ (αναλόγως των τιμών τής παραμέτρου k).

► **Εξέταση ειδικών περιπτώσεων με** $k < 0$. Όταν $k \in \{-1, -2, -3, -4\}$, ο προσδιορισμός τού συνόλου των ακεραίων λύσεων τής (5.132) διευκολύνεται αισθητά από το γεγονός ότι οι ακέραιες περιοχές

$$\mathfrak{O}_{-1} = \mathbb{Z}[i],\ \mathfrak{O}_{-2} = \mathbb{Z}[\sqrt{-2}] \text{ και } \mathfrak{O}_{-3} = \mathbb{Z}[\zeta_3],\ \text{όπου } \zeta_3 := \exp(\tfrac{2\pi i}{3}) = \tfrac{-1+\sqrt{-3}}{2},$$

είναι Π.Μ.Π. (Βλ. θεωρήματα 5.5.7 και 5.4.21, και πόρισμα 5.6.8.)

5.8.2 Θεώρημα. *Όταν $k = -1$, η μόνη λύση $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ τής εξισώσεως* (5.132) *είναι η* $(1, 0)$.

ΑΠΟΔΕΙΞΗ. Έστω $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ μια λύση τής (5.132) για $k = -1$. Εάν ο ακέραιος x ήταν άρτιος, τότε θα είχαμε

$$y^2 + 1 = x^3 \equiv 0 (\mathrm{mod}\, 8) \Rightarrow y^2 \equiv -1 \equiv 7 (\mathrm{mod}\, 8),$$

[78] Στη βιβλιογραφία συναντάται ενίοτε και ως *εξίσωση τού Bachet*, διότι ο Claude Gaspard Bachet de Méziriac (1581-1638) ήταν ο πρώτος που (το έτος 1621) βρήκε τις ακέραιες λύσεις της όταν $k = -2$. Ωστόσο, ήταν ο Louis Joel Mordell (1888-1972) εκείνος ο οποίος αφιέρωσε ένα μεγάλο μέρος των ερευνητικών του δραστηριοτήτων στη διεξοδική μελέτη της (για απειροπληθείς τιμές τής παραμέτρου k) και καταχώρισε ορισμένα από τα κύρια αποτελέσματά του στο κεφάλαιο 26 τού συγγράμματός του υπό τον τίλο *Diophantine Equations*, Academic Press, 1969.

[79] Βλ. L.J. Mordell: *Indeterminate equations of the third and fourth degree*, Quart. J. of Pure and Applied Math. **45** (1914), 170-186, και τού ιδίου: *A statement of Fermat*, Proc. London. Math. Soc. (2) **18** (1919), 5-6.

Προσοχή! Τούτο παύει να ισχύει για *ρητές λύσεις* τής (5.132). Επί παραδείγματι, για $k \notin \{1, -432\}$ και με τον k μη διαιρούμενο διά τής έκτης δυνάμεως ενός φυσικού αριθμού, είναι εύκολο να δειχθεί ότι η ύπαρξη *τουλάχιστον μίας* λύσεως $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ τής (5.132) συνεπιφέρει την ύπαρξη *απειροπληθών ρητών λύσεων*!

πράγμα αδύνατο[80]. Άρα ο x είναι περιττός και ο y άρτιος, και εντός τής Π.Μ.Π. $\mathbb{Z}[i]$ των γκαουσιανών ακεραίων ισχύει η ισότητα

$$(y+i)(y-i) = x^3. \tag{5.133}$$

Εάν $y \neq 0$, τότε $y+i, y-i \in \mathbb{Z}[i] \setminus \{\mathbb{Z}[i]^\times \cup \{0\}\}$ (διότι $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$) και είναι σχετικώς πρώτα. Πράγματι· εάν $d \in \text{ΜΚΔ}_{\mathbb{Z}[i]}(y+i, y-i)$, τότε

$$d \mid y \pm i \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(y \pm i) = y^2 + 1 = x^3 \equiv 1 (\mathrm{mod}\, 2),$$

$$d \mid (y+i) - (y-i) = 2i \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(2i) = 4,$$

οπότε ο (κατ' ανάγκην *περιττός*[81] μη αρνητικός[82] ακέραιος) $\mathbf{N}(d)$ ισούται με 1. (Ο μόνος περιττός μη αρνητικός ακέραιος διαιρέτης τού 4 είναι το 1.) Άρα $d \in \mathbb{Z}[i]^\times$ και, ως εκ τούτου, $d \underset{\text{συν.}}{\sim} 1$. (Βλ. 5.2.39 (vi) και 5.2.4 (iv).) Σημειωτέον ότι

$$1 = 1^3,\ -1 = (-1)^3,\ i = (-i)^3,\ -i = i^3.$$

Λόγω τής (5.133) το (ii) τού πορίσματος 5.6.15 εγγυάται την ύπαρξη ακεραίων a, b με $(a,b) \notin \{(0,0), (\pm 1, 0), (0, \pm 1)\}$ και τέτοιων, ώστε να ισχύει η ισότητα[83]

$$y + i = (a+bi)^3 = a\left(a^2 - 3b^2\right) + b\left(3a^2 - b^2\right) i,$$

από την οποία έπεται ότι

$$y = a\left(a^2 - 3b^2\right) \quad \text{και} \quad b\left(3a^2 - b^2\right) = 1.$$

Προφανώς, $b \in \{\pm 1\}$. Η τιμή $b = 1$ αποκλείεται (διότι η $3a^2 = 2$ δεν διαθέτει ακεραία λύση). Αυτό σημαίνει ότι $(a,b) = (0,-1)$. Όμως $(a,b) \neq (0,-1)$ (εξ υποθέσεως). Επομένως, $y = 0 \Rightarrow (x,y) = (1,0)$. □

5.8.3 Θεώρημα. *Όταν $k = -2$, οι μόνες λύσεις $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ τής* (5.132) *είναι οι*

$$(x,y) \in \{(3,5), (3,-5)\}.$$

ΑΠΟΔΕΙΞΗ. Έστω $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ μια λύση τής (5.132) για $k = -2$. Εάν ο ακέραιος x ήταν άρτιος, τότε θα είχαμε

$$y^2 + 2 = x^3 \equiv 0 (\mathrm{mod}\, 8) \Rightarrow y^2 \equiv -2 \equiv 6 (\mathrm{mod}\, 8),$$

[80] Εάν $y = 8\kappa + \lambda$, όπου $\kappa \in \mathbb{Z}$ και $\lambda \in \{0, \ldots, 7\}$, τότε $y^2 = 64\kappa^2 + 16\kappa\lambda + \lambda^2 \equiv \lambda^2 (\mathrm{mod}\, 8)$, όπου $\lambda^2 \equiv 0, 1$ ή $4 (\mathrm{mod}\, 8)$.

[81] Εάν το 2 διαιρούσε τον $\mathbf{N}(d)$, τότε θα έπρεπε να διαιρεί και τον x^3, πράγμα αδύνατο.

[82] Βλ. 5.2.39 (v).

[83] Σύμφωνα με το (ii) τού πορίσματος 5.6.15, *και* το $y - i$ μπορεί να παρασταθεί ως *κύβος* κάποιου στοιχείου τής Π.Μ.Π. $\mathbb{Z}[i]$. Ωστόσο, τούτο δεν θα το χρειασθούμε εδώ.

πράγμα αδύνατο (διότι $y^2 \equiv 0, 1$ ή $4 (\mathrm{mod}\, 8)$). Άρα αμφότεροι οι x και y είναι περιττοί, και εντός τής Π.Μ.Π. $\mathfrak{O}_{-2} = \mathbb{Z}[\sqrt{-2}]$ ισχύει η ισότητα

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3. \tag{5.134}$$

Επειδή $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$, τα $y \pm \sqrt{-2}$ ανήκουν στο $\mathbb{Z}[\sqrt{-2}] \setminus \{\mathbb{Z}[\sqrt{-2}]^\times \cup \{0\}\}$ και είναι σχετικώς πρώτα, διότι εάν $d \in \mathrm{MK}\Delta_{\mathbb{Z}[\sqrt{-2}]}(y + \sqrt{-2}, y - \sqrt{-2})$, τότε

$$d \mid y \pm \sqrt{-2} \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(y \pm \sqrt{-2}) = y^2 + 2 = x^3 \equiv 1 (\mathrm{mod}\, 2),$$

$$d \mid (y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2} \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(2\sqrt{-2}) = 8,$$

οπότε ο (κατ' ανάγκην *περιττός* μη αρνητικός ακέραιος) $\mathbf{N}(d)$ ισούται με 1. (Ο μόνος περιττός μη αρνητικός ακέραιος διαιρέτης τού 8 είναι το 1.) Άρα $d \in \mathbb{Z}[\sqrt{-2}]^\times$ και, ως εκ τούτου, $d \underset{\text{συν.}}{\sim} 1$. (Βλ. 5.2.39 (vi) και 5.2.4 (iv).) Σημειωτέον ότι $1 = 1^3, -1 = (-1)^3$. Λόγω τής (5.134) το (ii) τού πορίσματος 5.6.15 εγγυάται την ύπαρξη ακεραίων a, b με $(a, b) \notin \{(0, 0), (\pm 1, 0)\}$ και τέτοιων, ώστε να ισχύει η ισότητα

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 = a\left(a^2 - 6b^2\right) + b\left(3a^2 - 2b^2\right)\sqrt{-2},$$

από την οποία έπεται ότι

$$y = a\left(a^2 - 6b^2\right) \quad \text{και} \quad b\left(3a^2 - 2b^2\right) = 1.$$

Προφανώς, $b \in \{\pm 1\}$. Η τιμή $b = -1$ αποκλείεται (διότι $3a^2 - 2 = -1 \Rightarrow 3a^2 = 1$, όπου η τελευταία εξίσωση δεν διαθέτει ακεραία λύση). Αυτό σημαίνει ότι $b = 1$ και $3a^2 = 3 \Rightarrow a \in \{\pm 1\}$, οπότε $(x, y) \in \{(3, 5), (3, -5)\}$. □

5.8.4 Θεώρημα. *Όταν $k = -3$, η εξίσωση* (5.132) *δεν διαθέτει ακέραιες λύσεις.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι υπάρχει μια λύση $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ τής (5.132) για $k = -3$. Εάν ο ακέραιος x ήταν άρτιος, τότε θα είχαμε

$$y^2 + 3 = x^3 \equiv 0 (\mathrm{mod}\, 8) \Rightarrow y^2 \equiv -3 \equiv 5 (\mathrm{mod}\, 8),$$

πράγμα αδύνατο (διότι $y^2 \equiv 0, 1$ ή $4 (\mathrm{mod}\, 8)$). Άρα ο x είναι περιττός και ο y άρτιος. Μάλιστα, $x \equiv 3 (\mathrm{mod}\, 4)$, διότι[84]

$$y^2 \equiv 0 (\mathrm{mod}\, 4) \Rightarrow y^2 + 3 = x^3 \equiv 3 (\mathrm{mod}\, 4).$$

Θεωρούμε τον δακτύλιο

$$\mathfrak{O}_{-3} = \mathbb{Z}[\zeta_6] = \mathbb{Z}[-\zeta_3^2] = \left\{ a + \tfrac{1+\sqrt{-3}}{2} b \;\middle|\; a, b \in \mathbb{Z} \right\}$$

$$\underset{5.5.2}{=} \left\{ \tfrac{l+m\sqrt{-3}}{2} \;\middle|\; l, m \in \mathbb{Z} \text{ και } l \equiv m (\mathrm{mod}\, 2) \right\}$$

[84] Γράφοντας $x = 4l + m$, όπου $l \in \mathbb{Z}$ και $m \in \{0, 1, 2, 3\}$ λαμβάνουμε $x^3 = 4(16l^3 + 12l^2 m + 3lm^2) + m^3$, οπότε $m^3 \equiv 3 (\mathrm{mod}\, 4) \Rightarrow m = 3$.

των ακεραίων τού $\mathbb{Q}(\sqrt{-3})$, όπου $\zeta_3 := \exp(\frac{2\pi i}{3}) = \frac{-1+\sqrt{-3}}{2}$,

$$\zeta_6 := \exp(\tfrac{2\pi i}{3}) = \tfrac{1+\sqrt{-3}}{2} = -\zeta_3^2 \text{ και } \zeta_3^2 + \zeta_3 + 1 = 0.$$

Σημειωτέον ότι[85] $\mathfrak{O}_{-3} = \mathbb{Z}[\zeta_3]$ και[86]

$$\mathfrak{O}_{-3}^{\times} \underset{\text{5.5.3 (iii)}}{=} \left\{ \zeta_6^k \,\middle|\, k \in \{0,1,2,3,4,5\} \right\} = \left\{ \pm 1, \pm\zeta_3, \pm\zeta_3^2 \right\}.$$

Ο δακτύλιος $\mathfrak{O}_{-3}$, όντας **N**-ευκλείδεια περιοχή (κατά το θεώρημα 5.5.7), είναι Π.Κ.Ι. και, κατ' επέκταση, και Π.Μ.Π. (Βλ. θεώρημα 5.4.21 και πόρισμα 5.6.8.) Εντός τής Π.Μ.Π.[87] $\mathfrak{O}_{-3}$ ο κύβος x^3 παραγοντοποιείται ως ακολούθως:

$$(\underbrace{(y-1)+2\zeta_3}_{\in\mathfrak{O}_{-3}})(\underbrace{(y+1)-2\zeta_3}_{\in\mathfrak{O}_{-3}}) = (y+\sqrt{-3})(y-\sqrt{-3}) = y^2+3 = x^3, \quad (5.135)$$

όπου $y \pm \sqrt{-3} \in \mathfrak{O}_{-3} \setminus \{\mathfrak{O}_{-3}^{\times} \cup \{0\}\}$. Εάν $d \in \text{ΜΚΔ}_{\mathfrak{O}_{-3}}(y+\sqrt{-3}, y-\sqrt{-3})$, τότε

$$d \mid y \pm \sqrt{-3} \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(y \pm \sqrt{-3}) = y^2+3 = x^3 \equiv 1 (\mathrm{mod}\, 2),$$

$$d \mid (y+\sqrt{-3}) - (y-\sqrt{-3}) = 2\sqrt{-3} \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(2\sqrt{-3}) = 12,$$

οπότε ο (κατ' ανάγκην *περιττός* μη αρνητικός[88] ακέραιος) $\mathbf{N}(d)$ ισούται είτε με 1 είτε με 3. Ας υποθέσουμε ότι $\mathbf{N}(d) = 3$. Επειδή το 3 είναι πρώτος αριθμός, έχουμε

$$\left.\begin{array}{r} 3 \mid x^3 \underset{5.1.7}{\Longrightarrow} 3 \mid x \Rightarrow 3^2 \mid x^2 \\ x^2 \mid x^3 \end{array}\right\} \Rightarrow 3^2 \mid x^3 \quad (5.136)$$

και

$$3 \mid x^3 \Rightarrow 3 \mid x^3 - 3 = y^2 \underset{5.1.7}{\Longrightarrow} 3 \mid y \Rightarrow 3^2 \mid y^2. \quad (5.137)$$

Από τις (5.136) και (5.137) έπεται ότι $3^2 \mid x^3 - y^2 = 3$. Άτοπο! Κατά συνέπειαν,

$$\left.\begin{array}{l} \mathbf{N}(d) = 1 \underset{\text{5.5.3 (ii)}}{\Longrightarrow} d \in \mathfrak{O}_{-3}^{\times} \\ d = \underbrace{d}_{\in\mathfrak{O}_{-3}^{\times}} \cdot 1 \underset{5.2.5}{\Longrightarrow} d \underset{\text{συν.}}{\sim} 1 \end{array}\right\} \underset{5.2.12}{\Longrightarrow} 1 \in \text{ΜΚΔ}_{\mathfrak{O}_{-3}}(y+\sqrt{-3}, y-\sqrt{-3}),$$

δηλαδή τα $y+\sqrt{-3}, y-\sqrt{-3}$ είναι σχετικώς πρώτα. Λόγω τής (5.135) το (i) τού πορίσματος 5.6.15 εγγυάται την ύπαρξη ακεραίων l, m, με $(l,m) \notin \{(0,0), (\pm 2, 0)\}$

[85] Για οιουσδήποτε $a, b \in \mathbb{Z}$ έχουμε $a + b\zeta_3 = (a-b) + b(-\zeta_3^2) \in \mathfrak{O}_{-3}$, οπότε $\mathbb{Z}[\zeta_3] \subseteq \mathfrak{O}_{-3}$. Και αντιστρόφως· για οιουσδήποτε $c, d \in \mathbb{Z}$ έχουμε $c + d(-\zeta_3^2) = (c+d) + d\zeta_3 \in \mathbb{Z}[\zeta_3]$, οπότε $\mathfrak{O}_{-3} \subseteq \mathbb{Z}[\zeta_3]$.

[86] Προφανώς, $\zeta_6^0 = 1$, $\zeta_6^1 = -\zeta_3^2$, $\zeta_6^2 = \zeta_3$, $\zeta_6^3 = -1$, $\zeta_6^4 = \zeta_3^2$, $\zeta_6^5 = -\zeta_3$.

[87] Προσοχή! Η *γνήσια* υποπεριοχή $\mathbb{Z}[\sqrt{-3}]$ τής Π.Μ.Π. $\mathfrak{O}_{-3}$ είναι περιοχή με παραγοντοποίηση αλλά *δεν είναι* Π.Μ.Π. (Βλ. εδ. 5.6.7 (i).) Γι' αυτόν τον λόγο εργαζόμαστε με την $\mathfrak{O}_{-3}$.

[88] Βλ. (5.51).

και $l \equiv m(\mathrm{mod}\, 2)$, ήτοι αμφοτέρων αρτίων ή αμφοτέρων περιττών και τέτοιων, ώστε να ισχύει η ισότητα

$$y + \sqrt{-3} = \varepsilon \left(\tfrac{l+m\sqrt{-3}}{2}\right)^3 = \tfrac{\varepsilon}{8}\left((l^3 - 9lm^2) + 3(l^2m - m^3)\sqrt{-3}\right), \qquad (5.138)$$

για κάποιο $\varepsilon \in \mathfrak{O}_{-3}^{\times}$. Διακρίνουμε περιπτώσεις.

Περίπτωση πρώτη. Εάν $\varepsilon = \pm 1$, τότε εξισώνοντας τα φανταστικά μέρη στην (5.138) λαμβάνουμε $8 = \pm 3(l^2m - m^3) \Rightarrow 3 \mid 8$. Άτοπο!

Περίπτωση δεύτερη. Εάν $\varepsilon \in \left\{-\zeta_3, -\zeta_3^2\right\}$, ήτοι $\varepsilon = \frac{1\pm\sqrt{-3}}{2}$, τότε εξισώνοντας εκ νέου τα φανταστικά μέρη στην (5.138) λαμβάνουμε

$$16 = \pm(l^3 - 9lm^2) + 3(l^2m - m^3) = ((\pm l) + m)^3 - 12(\pm l)m^2 - 4m^3.$$

Επειδή $l \equiv m(\mathrm{mod}\, 2)$, έχουμε $(\pm l) + m \equiv 0(\mathrm{mod}\, 2) \Rightarrow \exists u \in \mathbb{Z} : (\pm l) + m = 2u$, οπότε

$$16 = (2u)^3 - 12(2u - m)m^2 - 4m^3 \Rightarrow 2 = u^3 - 3m^2u + m^3. \qquad (5.139)$$

Εάν *είτε* ο ένας εκ των ακεραίων u, m είναι άρτιος και ο άλλος περιττός *είτε* αμφότεροι οι u, m είναι περιττοί, η (5.139) είναι αναληθής, καθώς το δεξιό της μέλος θα είναι ένας περιττός ακέραιος. Άρα αμφότεροι οι u, m είναι άρτιοι. Όμως τούτο σημαίνει ότι το δεξιό μέλος τής (5.139) θα διαιρείται διά τού 8. Άτοπο!

Περίπτωση τρίτη. Εάν $\varepsilon \in \left\{\zeta_3, \zeta_3^2\right\}$, ήτοι $\varepsilon = \frac{-1\pm\sqrt{-3}}{2}$, τότε εξισώνοντας τα φανταστικά μέρη στην (5.138) λαμβάνουμε

$$16 = \pm(l^3 - 9lm^2) - 3(l^2m - m^3) = ((\pm l) + m)^3 - 12(\pm l)m^2 - 6l^2m + 2m^3.$$

Επειδή $l \equiv m(\mathrm{mod}\, 2)$, έχουμε $(\pm l) + m \equiv 0(\mathrm{mod}\, 2) \Rightarrow \exists u \in \mathbb{Z} : (\pm l) + m = 2u$, οπότε

$$\begin{aligned} &16 = (2u)^3 - 12(2u - m)m^2 - 6(2u - m)^2m + 2m^3 \\ &\Rightarrow 2 = u^3 - 3mu^2 + m^3 \end{aligned}$$

και μέσω των επιχειρημάτων που χρησιμοποιήθηκαν στη δεύτερη περίπτωση καταλήγουμε εκ νέου σε άτοπο! Άρα η εξίσωση (5.132) τού Mordell δεν διαθέτει ακέραιες λύσεις όταν $k = -3$. □

5.8.5 Θεώρημα. *Όταν $k = -4$, οι μόνες λύσεις $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ τής* (5.132) *είναι οι*

$$(x, y) \in \{(2, \pm 2), (5, \pm 11)\}.$$

ΑΠΟΔΕΙΞΗ. Έστω $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ μια λύση τής (5.132) για $k = -4$. Επειδή

$$y^2 + 4 = x^3 \Rightarrow y^2 \equiv x^3(\mathrm{mod}\, 2),$$

είτε αμφότεροι οι x, y είναι περιττοί είτε αμφότεροι είναι άρτιοι.

Περίπτωση πρώτη. Εάν αμφότεροι οι x, y είναι *περιττοί*, τότε εντός τής Π.Μ.Π. $\mathbb{Z}[i]$ των γκαουσιανών ακεραίων ισχύει η ισότητα

$$(y + 2i)(y - 2i) = x^3. \tag{5.140}$$

Τα στοιχεία $y + 2i, y - 2i$ ανήκουν στο $\mathbb{Z}[i] \setminus \{\mathbb{Z}[i]^\times \cup \{0\}\}$ (διότι $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$) και είναι σχετικώς πρώτα. Πράγματι· εάν $d \in \text{ΜΚΔ}_{\mathbb{Z}[i]}(y + i, y - i)$, τότε

$$d \mid y + 2i \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(y + 2i) = y^2 + 4 = x^3 \equiv 1 (\mathrm{mod}\, 2),$$

$$d \mid (y + 2i) - (y - 2i) = 4i \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(4i) = 16,$$

οπότε ο (κατ' ανάγκην *περιττός* μη αρνητικός ακέραιος) $\mathbf{N}(d)$ ισούται με 1. (Ο μόνος περιττός μη αρνητικός ακέραιος διαιρέτης τού 16 είναι το 1.) Άρα $d \in \mathbb{Z}[i]^\times$ και, ως εκ τούτου, $d \underset{\text{συν.}}{\sim} 1$. (Βλ. 5.2.39 (vi) και 5.2.4 (iv).) Σημειωτέον ότι

$$1 = 1^3,\ -1 = (-1)^3,\ i = (-i)^3,\ -i = i^3. \tag{5.141}$$

Λόγω τής (5.140) το (ii) τού πορίσματος 5.6.15 εγγυάται την ύπαρξη ακεραίων a, b με $(a, b) \notin \{(0, 0), (\pm 1, 0), (0, \pm 1)\}$ και τέτοιων, ώστε να ισχύει η ισότητα

$$y + 2i = (a + bi)^3 = a\left(a^2 - 3b^2\right) + b\left(3a^2 - b^2\right) i,$$

από την οποία έπεται ότι

$$y = a\left(a^2 - 6b^2\right) \quad \text{και} \quad b\left(3a^2 - b^2\right) = 2.$$

Από τη δεύτερη εξίσωση συνάγεται ότι $b \in \{\pm 1, \pm 2\}$. Οι τιμές $b = 2$, $b = -1$ και $b = 1$ αποκλείονται (οι πρώτες δύο διότι οι $3a^2 = 5$ και $3a^2 = -1$ δεν διαθέτουν ακεραία λύση και η τρίτη διότι ο y θα όφειλε να είναι άρτιος). Για $b = -2$ λαμβάνουμε

$$a = \pm 1 \Rightarrow (x, y) \in \{(5, 11), (5, -11)\}.$$

Περίπτωση δεύτερη. Εάν αμφότεροι οι x, y είναι *άρτιοι*, τότε $x = 2x'$ και $y = 2y'$ για κάποιους $x', y' \in \mathbb{Z}$, οπότε

$$(2y')^2 + 4 = (2x')^3 \Rightarrow {y'}^2 + 1 = 2{x'}^3 \tag{5.142}$$

και εντός τής Π.Μ.Π. $\mathbb{Z}[i]$ των γκαουσιανών ακεραίων ισχύει η ισότητα

$$(y' + i)(y' - i) = 2{x'}^3.$$

Εάν $d \in \text{ΜΚΔ}_{\mathbb{Z}[i]}(y' + i, y' - i)$, τότε $d \mid (y' + i) - (y' - i) = 2i = (1 + i)^2$, οπότε $dz = (1 + i)^2$ για κάποιον $z \in \mathbb{Z}[i]$. Το $1 + i$ είναι ανάγωγο στοιχείο τής Π.Μ.Π.

$\mathbb{Z}[i]$ (διότι $\mathbf{N}(1+i)=2$, βλ. πρόταση 5.3.9). Επομένως, το d είναι συντροφικό με ένα εκ των στοιχείων $1, i+1$ ή $(1+i)^2$. Το $i+1$ διαιρεί αμφότερα τα $y'+i$ και $y'-i$, διότι

$$y' \pm i = (\underbrace{\tfrac{1+y'}{2}}_{\in\mathbb{Z}} \pm \underbrace{\tfrac{1-y'}{2}}_{\in\mathbb{Z}} i)(i+1),$$

οπότε $d \underset{\text{συν.}}{\nsim} 1$, διότι $i+1 \notin \mathbb{Z}[i]$. (Βλ. λήμμα 5.2.27 και πρόταση 5.2.12.) Από την άλλη μεριά, το $(1+i)^2$ δεν είναι κοινός διαιρέτης των $y'+i$ και $y'-i$, διότι εάν ίσχυε

$$(1+i)^2 \mid y'+i = (\underbrace{\tfrac{1+y'}{2}}_{\in\mathbb{Z}} + \underbrace{\tfrac{1-y'}{2}}_{\in\mathbb{Z}} i)(i+1) \Rightarrow 1+i \mid \tfrac{1+y'}{2} + \tfrac{1-y'}{2} i,$$

θα υπήρχαν $\nu, \xi \in \mathbb{Z}$ με

$$\begin{aligned} &\tfrac{1+y'}{2} + \tfrac{1-y'}{2} i = (1+i)(\nu+\xi i) = \nu - \xi + (\xi+\nu)\, i \\ &\Rightarrow [1+y' = 2(\nu-\xi), 1-y' = 2\,(\xi+\nu)] \Rightarrow 2\nu = 1, \end{aligned}$$

πράγμα αδύνατο. Άρα $d \underset{\text{συν.}}{\sim} i+1$. Το $i+1$ είναι ένας μέγιστος κοινός διαιρέτης των $y'+i$ και $y'-i$, και

$$y'+i = (i+1)(a+bi) \;\text{ και }\; y'-i = (i+1)(c+di), \tag{5.143}$$

όπου τα $a+bi, c+di \in \mathbb{Z}[i]$ είναι σχετικώς πρώτα. (Βλ. πρόταση 5.2.12 και λήμμα 5.2.28.) Κατά συνέπειαν,

$$2x'^3 = (y'+i)(y'-i) = (1+i)^2(a+bi)(c+di) = 2i(a+bi)(c+di),$$

απ' όπου έπεται ότι

$$(a+bi)(c+di) = \tfrac{1}{i} x'^3 = (-i)x'^3 = (ix')^3. \tag{5.144}$$

Προφανώς, $(a,b) \notin \{(0,0),(-1,0)\}$ (από την πρώτη εκ των (5.143)). Επιπροσθέτως, στην περίπτωση κατά την οποία $(a,b) = (1,0)$ έχουμε $c=0$, $x'^3 = -d$ και $y'=1$, οπότε

$$1 = y'^2 = 2x'^3 - 1 \Rightarrow x'^3 = 1 = -d \Rightarrow x' = 1 \Rightarrow (x,y) = (2,2).$$

Εάν $(a,b) \notin \{(1,0),(0,\pm 1)\}$, τότε λόγω των (5.144) και (5.141) το (ii) τού πορίσματος 5.6.15 εγγυάται την ύπαρξη ακεραίων l, m με $(l,m) \notin \{(0,0),(\pm 1,0),(0,\pm 1)\}$ και τέτοιων, ώστε να ισχύει

$$\begin{aligned} a+bi &= \tfrac{y'+i}{i+1} = (l+mi)^3 \\ \Rightarrow y'+i &= (l^3 - 3lm^2 - 3l^2m + m^3) + (l^3 - 3lm^2 + 3l^2m - m^3)i \end{aligned}$$

ή, ισοδυνάμως,

$$\left\{ \begin{array}{l} y' = l^3 - 3lm^2 - 3l^2m + m^3 = (l+m)(l^2 - 4lm + m^2), \\ 1 = l^3 - 3lm^2 + 3l^2m - m^3 = (l-m)(l^2 + 4lm + m^2). \end{array} \right\}$$

Από τη δεύτερη εξίσωση συνάγεται ότι είτε

$$[l - m = -1 \text{ και } l^2 + 4lm + m^2 = -1] \text{ είτε } [l - m = 1 \text{ και } l^2 + 4lm + m^2 = 1].$$

Το πρώτο ενδεχόμενο αποκλείεται (διότι εν τοιαύτη περιπτώσει $m \notin \mathbb{Z}$). Άρα $l - m = 1$ και

$$m \in \{-1, 0\} \Rightarrow (l, m) \in \{(0, -1), (1, 0)\}.$$

Άτοπο! Άρα $(a, b) \in \{(1, 0), (0, \pm 1)\}$. Εάν $a = 0$, τότε (από την πρώτη εκ των (5.143)) λαμβάνουμε

$$[b = 1 \text{ και } y' = -1] \underset{(5.142)}{\Longrightarrow} x' = 1 \Rightarrow (x, y) = (2, -2).$$

Εάν $a = 1$ και $b = 0$, τότε (από την πρώτη εκ των (5.143)) λαμβάνουμε $y' = 1$ και από την (5.142) έπεται εκ νέου ότι $(x, y) = (2, -2)$. □

5.8.6 Σημείωση. (i) Για έναν ακέραιο $m \leq -1$ στερούμενον τετραγώνων η ακεραία περιοχή $\mathfrak{O}_m$ (σύμφωνα με τα θεωρήματα 5.5.14 και 5.6.10) είναι Π.Μ.Π. μόνον όταν

$$m \in \{-163, -67, -43, -19, -11, -7, -3, -2, -1\}.$$

Για αυτές τις εννέα τιμές τού m η εξίσωση (5.132) τού Mordell έχουσα παράμετρο $k = ml^2$ (για κάποιον $l \in \mathbb{N}$) μας επιτρέπει την παραγοντοποίηση

$$x^3 = y^2 - k = y^2 - (l\sqrt{m})^2 = (\underbrace{y - l\sqrt{m}}_{\in \mathfrak{O}_m})(\underbrace{y + l\sqrt{m}}_{\in \mathfrak{O}_m})$$

τού κύβου x^3 εντός τής $\mathfrak{O}_m$ (ή κάποιες παρόμοιες, όπως, π.χ., στη δεύτερη περίπτωση τής αποδείξεως τού θεωρήματος 5.8.5). Τούτο, σε συνδυασμό με ορισμένα ενδιάμεσα στοιχειώδη αριθμοθεωρητικά επιχειρήματα και με το ότι η $\mathfrak{O}_m^\times$ είναι γνωστή, μας επιτρέπει, όταν τα στοιχεία $y - l\sqrt{m}$ και $y + l\sqrt{m}$ είναι πρώτα μεταξύ τους εντός τής $\mathfrak{O}_m$, την εφαρμογή τού πορίσματος 5.6.15 κατά την αναζήτηση τυχόν ακεραίων λύσεων $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ τής (5.132). Ωστόσο, ενδέχεται οι απαιτούμενοι υπολογισμοί να είναι αρκετά περίπλοκοι (όπως, π.χ., όταν[89] $k = -18 = -2 \cdot 3^2$ ή όταν[90] $k = -28 = -7 \cdot 2^2$) ή/και να καταλήγουν σε άλλες διοφαντικές εξισώσεις

[89] Βλ. R. Finkelstein & H. London: *On Mordell's equation* $y^2 - k = x^3$. *An interesting case of Sierpinski*, Journal of Number Theory **2** (1970), 310-321.

[90] Βλ. W.J. Ellison, F. Ellison, J. Pesek, C.E. Stahl & D. Stall: *The diophantine equation* $y^2 + k = x^3$, Journal of Number Theory **4** (1972), 107-117.

(όχι πάντοτε αναγόμενες στη μελέτη παραγοντοποιήσεων εντός κάποιας, έστω και διαφορετικής, Π.Μ.Π.). Επιπροσθέτως, όταν ο k δεν είναι τής μορφής $k = ml^2$, το ανωτέρω τέχνασμα δεν είναι εφαρμόσιμο. Εν τοιαύτη περιπτώσει, είναι απαραίτητη η χρήση είτε κατάλληλων *γενικεύσεων* τού πορίσματος 5.6.15 (για ακέραιες περιοχές που δεν είναι κατ' ανάγκην Π.Μ.Π.) είτε άλλων αλγεβρικών ή/και γεωμετρικών μεθόδων (π.χ., από τη Θεωρία των Ελλειπτικών Καμπυλών κ.ά.).

(ii) Στον κάτωθι κατάλογο έχουν καταχωρισθεί οι τιμές τής παραμέτρου k με $-50 \leq k \leq -1$, για τις οποίες η εξίσωση (5.132) τού Mordell διαθέτει ακέραιες λύσεις, καθώς και οι ίδιες οι λύσεις.

k	$(x, \pm y)$
-1	$(1, 0)$
-2	$(3, 5)$
-4	$(2, 2), (5, 11)$
-7	$(2, 1), (32, 181)$
-8	$(2, 0)$
-11	$(3, 4), (15, 58)$
-13	$(17, 70)$
-15	$(4, 7)$
-18	$(3, 3)$
-19	$(7, 18)$
-20	$(6, 14)$
-23	$(3, 2)$

k	$(x, \pm y)$
-25	$(5, 10)$
-26	$(3, 1), (35, 207)$
-27	$(3, 0)$
-28	$(4, 6), (8, 22), (37, 225)$
-35	$(11, 36)$
-39	$(4, 5), (10, 31), (22, 103)$
-40	$(14, 52)$
-44	$(5, 9)$
-45	$(21, 96)$
-47	$(6, 13), (12, 41), (63, 500)$
-48	$(4, 4), (28, 148)$
-49	$(65, 524)$

► **Εξέταση ειδικών περιπτώσεων με παράμετρο** $k > 0$. Δειγματοληπτικώς, στο θεώρημα 5.8.9 προσδιορίζονται όλες οι ακέραιες λύσεις τής εξισώσεως (5.132) όταν $k = 1$, ενώ μέσω τού θεωρήματος 5.8.10 αποδεικνύεται η μη ύπαρξη ακεραίων λύσεων όταν $k = 6$.

5.8.7 Θεώρημα. *Η εξίσωση* $x^3 + z^3 = 2y^3$ *δεν διαθέτει λύσεις* $(x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ *όταν* $x \neq z$ *και* $y \neq 0$.

ΑΠΟΔΕΙΞΗ. Μια απόδειξη εντοπίζεται στο βιβλίο των «Στοιχείων τής Άλγεβρας» τού L. Euler[91] (που είχε πρωτοδημοσιευθεί το 1770). Για άλλη μία (παρόμοια αλλά λεπτομερέστερη) απόδειξη με στοιχειώδη μέσα (οφειλόμενη στον A. Waculicz[92]) βλ. W. Sierpinski: *Elementary Theory of Numbers*, North Holland, 1991, Thm. 9, pp. 77-78. □

5.8.8 Πόρισμα. *Οι μόνες λύσεις* $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ *τής εξισώσεως* $x^3 - 2y^3 = 1$ *είναι οι*

$$(x, y) \in \{(1, 0), (-1, -1)\}.$$

[91] Βλ. L. Euler: *Elements of Algebra*, translated by J. Hewlett, reprinted from the fifth ed. (Longman, Orman and Co., 1840), with an introduction by C. Truesdell, Springer-Verlag, 1972, θεώρημα τού εδ. 247, σελ. 456-468.

[92] A. Waculicz: *On the equation* $x^3 + y^3 = 2z^3$, Colloq. Math. **5** (1957), 11-15.

ΑΠΟΔΕΙΞΗ. Εάν $x^3-2y^3=1$ για κάποιο ζεύγος $(x,y)\in\mathbb{Z}\times\mathbb{Z}$, τότε (σύμφωνα με το θεώρημα 5.8.7, εφαρμοζόμενο για $z=-1$) *είτε* $x=-1$ (οπότε $y^3=-1\Rightarrow y=-1$) *είτε* $y=0$ (οπότε $x^3=1\Rightarrow x=1$). □

5.8.9 Θεώρημα. *Όταν* $k=1$, *οι μόνες λύσεις* $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ *της εξισώσεως* (5.132) *είναι οι*

$$(x,y)\in\{(-1,0),(0,\pm1),(2,\pm3)\}.$$

ΑΠΟΔΕΙΞΗ. Έστω $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ μια λύση τής (5.132) για $k=1$. Τότε

$$y^2-1=(y+1)(y-1)=x^3. \tag{5.145}$$

Επειδή $(y+1)-(y-1)=2$, έχουμε μκδ$(y+1,y-1)\in\{1,2\}$.

Περίπτωση πρώτη. Εάν $y=0$, τότε η (5.145) δίδει $x=-1$. Επίσης (λόγω τής (5.145)) οι τιμές $y=\pm2$ είναι αδύνατες.

Περίπτωση δεύτερη. Ας υποθέσουμε ότι $y\notin\{0,\pm2\}$ και ότι ο y είναι *άρτιος*. Τότε $y+1\neq\pm1$, $y-1\neq\pm1$ και μκδ$(y+1,y-1)=1$. Επειδή $\mathbb{Z}^\times=\{\pm1\}$ και $1^3=1$, $(-1)^3=-1$, το (ii) τού πορίσματος 5.6.15 εγγυάται (λόγω τής (5.145) και τού ότι ο δακτύλιος $\mathbb{Z}$ είναι Π.Μ.Π.) την ύπαρξη ακεραίων $a\neq\pm1, b\neq\pm1$, τέτοιων ώστε να ισχύουν οι ισότητες $y+1=a^3$ και $y-1=b^3$. Εξ αυτών συνάγεται ότι

$$2=a^3-b^3=(a-b)\left(a^2+ab+b^2\right)\Rightarrow[a-b=\pm2\ \text{ και }\ a^2+ab+b^2=\pm1],$$

διότι αμφότεροι οι a,b είναι κατ' ανάγκην περιττοί. Τούτο είναι αδύνατο με το πρόσημο $-$, διότι εν τοιαύτη περιπτώσει

$$a=b-2\Rightarrow 3b^2-6b+5=0\Rightarrow b=1\pm\tfrac{1}{3}\sqrt{-6}\notin\mathbb{Z}.$$

Με το πρόσημο $+$ λαμβάνουμε

$$a=b+2\Rightarrow 3b^2+6b+4=1\Rightarrow(b+1)^2=0\Rightarrow(a,b)=(1,-1),$$

Τούτο είναι εκ νέου αδύνατο, διότι εξ υποθέσεως $a\neq\pm1$ και $b\neq\pm1$.

Περίπτωση τρίτη. Εάν $y\in\{\pm1,\pm3,\pm5\}$, τότε από την (5.145) βλέπουμε ότι οι τιμές $y=\pm5$ είναι αδύνατες, ενώ για τις λοιπές λαμβάνουμε

$$(x,y)\in\{(0,\pm1),(2,\pm3)\}.$$

Περίπτωση τέταρτη. Ας υποθέσουμε ότι $y\notin\{\pm1,\pm3,\pm5\}$ και ότι ο y είναι *περιττός*. Τότε ο x είναι άρτιος, $y\equiv1$ ή $3\pmod4$ και

$$\text{μκδ}(y+1,y-1)=2\Rightarrow\text{μκδ}(\tfrac{y+1}{2},\tfrac{y-1}{2})=1.$$

(i) Εάν $y\equiv1\pmod4$, τότε ισχύει η ισότητα

$$\left(\tfrac{1}{2}x\right)^3=\tfrac{y+1}{2}\tfrac{y-1}{4}\ \text{ με }\ \tfrac{y+1}{2}\neq\pm1,\ \tfrac{y-1}{4}\neq\pm1$$

και μκδ$(\frac{y+1}{2}, 2(\frac{1}{4}(y-1))) = 1 \Rightarrow$ μκδ$(\frac{y+1}{2}, \frac{y-1}{4}) = 1$. Από το (ii) τού πορίσματος 5.6.15 έπεται ότι

$$\exists (a,b) \in (\mathbb{Z} \setminus \{\pm 1\}) \times (\mathbb{Z} \setminus \{\pm 1\}) : \left[\tfrac{y+1}{2} = a^3 \text{ και } \tfrac{y-1}{4} = b^3\right],$$

και, κατ' επέκταση, ότι

$$2a^3 - 1 = y = 4b^3 + 1 \Rightarrow a^3 - 2b^3 = 1.$$

Σύμφωνα με το πόρισμα 5.8.8, $(a,b) \in \{(1,0), (-1,-1)\}$. Άτοπο!

(ii) Εάν $y \equiv 3 (\mathrm{mod}\, 4)$, τότε $-y \equiv 1 (\mathrm{mod}\, 4)$, οπότε

$$\left(\tfrac{1}{2}x\right)^3 = \tfrac{(-y)+1}{2}\tfrac{(-y)-1}{4} \text{ με } \tfrac{(-y)+1}{2} \neq \pm 1,\ \tfrac{(-y)-1}{4} \neq \pm 1$$

και επαναλαμβάνοντας την ίδια επιχειρηματολογία με το $-y$ στη θέση τού y καταλήγουμε εκ νέου σε άτοπο. □

5.8.10 Θεώρημα. *Όταν $k = 6$, η εξίσωση* (5.132) *δεν διαθέτει ακέραιες λύσεις.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι υπάρχει μια λύση $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ τής (5.132) για $k = 6$. Εάν ο ακέραιος x ήταν άρτιος, τότε θα είχαμε

$$y^2 - 6 = x^3 \equiv 0 (\mathrm{mod}\, 8) \Rightarrow y^2 \equiv 6 (\mathrm{mod}\, 8),$$

πράγμα αδύνατο (διότι $y^2 \equiv 0, 1$ ή $4 (\mathrm{mod}\, 8)$). Άρα αμφότεροι οι x και y είναι *περιττοί* και[93]

$$y^2 \equiv 1 (\mathrm{mod}\, 8) \Rightarrow x^3 = y^2 - 6 \equiv -5 \equiv 3 (\mathrm{mod}\, 8) \Rightarrow x \equiv 3 (\mathrm{mod}\, 8).$$

Γράφοντας την $y^2 = x^3 + 6$ ως $y^2 + 2 = x^3 + 8 = (x+2)(x^2 - 2x + 4)$ παρατηρούμε ότι $y^2 + 2 \equiv 3 (\mathrm{mod}\, 8)$ και

$$x^2 - 2x + 4 \equiv 3^2 - 2 \cdot 3 + 4 \equiv 7 (\mathrm{mod}\, 8). \tag{5.146}$$

Έστω p ένας πρώτος αριθμός που διαιρεί τον παράγοντα $x^2 - 2x + 4$. Τότε $p \neq 2$ (διότι ο x είναι περιττός) και

$$p \mid y^2 + 2 \Rightarrow y^2 \equiv -2 (\mathrm{mod}\, p) \Leftrightarrow \left(\tfrac{-2}{p}\right) = 1 \underset{(5.92)}{\Longleftrightarrow} p \equiv 1 \text{ ή } 3 (\mathrm{mod}\, 8).$$

Επειδή $x^2 - 2x + 4 = (x-1)^2 + 3 \geq 3$, έχουμε[94]

$$\left.\begin{array}{c} x^2 - 2x + 4 = p_1 \cdots p_\nu \\ \text{για κάποιους πρώτους} \\ \text{αριθμούς } p_1, \ldots, p_\nu\ (\nu \in \mathbb{N}) \\ \text{με } p_j \equiv 1 \text{ ή } 3 (\mathrm{mod}\, 8), \forall j \in \{1, \ldots, \nu\} \end{array}\right\} \Rightarrow x^2 - 2x + 4 \equiv 1 \text{ ή } 3 (\mathrm{mod}\, 8). \tag{5.147}$$

Από τις (5.146) και (5.147) καταλήγουμε σε άτοπο! □

[93] Γράφοντας $x = 8q + r$, όπου $q \in \mathbb{Z}$ και $r \in \{0, 1, \ldots, 7\}$ λαμβάνουμε $x^3 = (8q + r)^3 \equiv r^3 (\mathrm{mod}\, 8)$. Επειδή $r^3 \equiv 3 (\mathrm{mod}\, 8)$, συμπεραίνουμε ότι $r = 3$.

[94] Προφανώς $p_1 \cdots p_\nu \equiv 3^\kappa (\mathrm{mod}\, 8)$ για κάποιον $\kappa \in \{0, 1, \ldots, \nu\}$. Εάν $\kappa \geq 2$, τότε $p_1 \cdots p_\nu \equiv 9^{\frac{\kappa}{2}} \equiv 1 (\mathrm{mod}\, 8)$ όταν ο κ είναι άρτιος και $p_1 \cdots p_\nu \equiv 9^{\frac{\kappa-1}{2}} \cdot 3 \equiv 3 (\mathrm{mod}\, 8)$ όταν ο κ είναι περιττός.

5.8.11 Σημείωση. Στον κάτωθι κατάλογο έχουν καταχωρισθεί οι τιμές τής παραμέτρου k με $1 \leq k \leq 50$, για τις οποίες η εξίσωση (5.132) τού Mordell διαθέτει ακέραιες λύσεις, καθώς και οι ίδιες οι λύσεις.

k	$(x, \pm y)$
1	$(-1,0), (0,1), (2,3)$
2	$(-1,1)$
3	$(1,2)$
4	$(0,2)$
5	$(-1,2)$
8	$(-2,0), (1,3), (2,4), (46,312)$
9	$(-2,1), (0,3), (3,6), (6,15), (40,253)$
10	$(-1,3)$
12	$(-2,2), (13,47)$
15	$(1,4), (109,1138)$
16	$(0,4)$
17	$(-2,3), (-1,4), (2,5), (4,9), (8,23),$ $(43,282), (52,375), (5234,378661)$
18	$(7,19)$
19	$(5,12)$
22	$(3,7)$
24	$(-2,4), (1,5), (10,32), (8158,736844)$
25	$(0,5)$

k	$(x, \pm y)$
26	$(-1,5)$
27	$(-3,0)$
28	$(-3,1), (2,6)$
30	$(19,83)$
31	$(-3,2)$
33	$(-2,5)$
35	$(1,6)$
36	$(-3,3), (0,6),$ $(4,10), (12,42)$
37	$(-1,6), (3,8), (243,3788)$
38	$(11,37)$
40	$(6,16)$
41	$(2,7)$
43	$(-3,4)$
44	$(-2,6), (5,13)$
48	$(1,7)$
49	$(0,7)$
50	$(-1,7)$

► **Θεωρήματα που αφορούν στη μη ύπαρξη ακεραίων λύσεων.** Ακόμη και μέσω των ήδη παρατεθέντων καταλόγων (στα εδ. 5.8.6 (ii) και 5.8.11) μπορεί κανείς να εικάσει ότι υφίστανται ολόκληρες *οικογένειες τιμών* τής παραμέτρου k για τις οποίες το σύνολο των ακεραίων λύσεων τής εξισώσεως (5.132) είναι κενό. Τα θεωρήματα 5.8.12, 5.8.14 και 5.8.16 περιγράφουν ορισμένες εξ αυτών των οικογενειών.

5.8.12 Θεώρημα. *Εάν $a, b \in \mathbb{Z}$, τότε η εξίσωση* (5.132) *με παράμετρο k δεν διαθέτει ακέραιες λύσεις στις ακόλουθες περιπτώσεις*:

(i) $k = a^3 - 4b^2$, *όπου* $a \equiv 3 (\mathrm{mod}\, 4)$ *και* $p \not\equiv 3 (\mathrm{mod}\, 4)$ *για κάθε πρώτον αριθμό* p *με* $p \mid b$.

(ii) $k = a^3 - b^2$, *όπου* $a \equiv 2 (\mathrm{mod}\, 4)$, $b \equiv 1 (\mathrm{mod}\, 2)$ *και* $p \not\equiv 3 (\mathrm{mod}\, 4)$ *για κάθε πρώτον αριθμό* p *με* $p \mid b$.

ΑΠΟΔΕΙΞΗ. (i) Ας υποθέσουμε ότι υπάρχει μια λύση $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ τής (5.132). Γράφοντας την (5.132) ως

$$y^2 + 4b^2 = x^3 + a^3 \tag{5.148}$$

και εργαζόμενοι $\mathrm{mod}\, 4$ παρατηρούμε ότι το αριστερό μέλος τής (5.148) είναι $\equiv 0$ ή $1 (\mathrm{mod}\, 4)$, ενώ το δεξιό μέλος είναι[95] $\equiv 0, 2$ ή $3 (\mathrm{mod}\, 4)$. Άρα αμφότερα τα μέλη

[95] Προφανώς, $a^3 \equiv 3 (\mathrm{mod}\, 4)$ και γράφοντας $x = 4\kappa + \lambda$, για κάποιους $\kappa \in \mathbb{Z}$ και $\lambda \in \{0, 1, 2, 3\}$ λαμβάνουμε $x^3 = 64\kappa^3 + 48\kappa^2\lambda + 12\kappa\lambda^2 + \lambda^3 \equiv \lambda^3 (\mathrm{mod}\, 8)$, όπου $\lambda^3 \equiv 0, 1$ ή $3 (\mathrm{mod}\, 4)$.

είναι $\equiv 0(\mathrm{mod}\,4)$, απ' όπου έπεται ότι ο y είναι *άρτιος* και $x \equiv 1(\mathrm{mod}\,4)$. Παραγοντοποίηση τού δεξιού μέλους τής (5.148) δίδει

$$y^2 + 4b^2 = (x+a)(x^2 - ax + a^2), \tag{5.149}$$

όπου

$$x^2 - ax + a^2 \equiv 1^2 - 3 \cdot 1 + 3^2 \equiv 3(\mathrm{mod}\,4). \tag{5.150}$$

Προφανώς, λόγω τής (5.150), $2 \nmid x^2 - ax + a^2$ και $x^2 - ax + a^2 \notin \{\pm 1, \pm 2\}$. Ως εκ τούτου, οι πρώτοι αριθμοί που διαιρούν τον παράγοντα $x^2 - ax + a^2$ είναι περιττοί και $\equiv 1$ ή $3(\mathrm{mod}\,4)$. Επιπροσθέτως, *τουλάχιστον ένας* εξ αυτών οφείλει να είναι $\equiv 3(\mathrm{mod}\,4)$. Έστω, λοιπόν, p ένας πρώτος αριθμός με

$$p \mid x^2 - ax + a^2 \underset{(5.149)}{\Longrightarrow} p \mid y^2 + 4b^2 \tag{5.151}$$

και $p \equiv 3(\mathrm{mod}\,4)$. Εξ υποθέσεως, $p \nmid b$, οπότε $p \nmid 4b^2$. Από την (5.151) έπεται ότι

$$y^2 \equiv -4b^2(\mathrm{mod}\,p) \Leftrightarrow 1 = \left(\tfrac{-4b^2}{p}\right) = \left(\tfrac{(2b)^2}{p}\right)\left(\tfrac{-1}{p}\right) = \left(\tfrac{-1}{p}\right) \underset{(5.91)}{\Longleftrightarrow} p \equiv 1(\mathrm{mod}\,4),$$

κάτι που αντίκειται στο ότι (εξ υποθέσεως) $p \equiv 3(\mathrm{mod}\,4)$.

(ii) Τούτο είναι παρόμοιο, καθώς *και σε αυτήν την περίπτωση*, εάν $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ ήταν μια υποτιθέμενη λύση τής εξισώσεως (5.132), θα είχαμε $x \equiv 1(\mathrm{mod}\,4)$ και $x^2 - ax + a^2 \equiv 3(\mathrm{mod}\,4)$, απ' όπου θα καταλήγαμε σε άτοπο. □

5.8.13 Παρατήρηση. Για $|k| \leq 50$ το θεώρημα 5.8.12 αποκλείει την ύπαρξη ακεραίων λύσεων τής (5.132) όταν

$$k \in \{-41, -33, -17, -9, -5, 7, 11, 23, 39, 47\}.$$

Παρεμφερή (αν και κατά τι γενικότερης φύσεως) είναι τα δύο θεωρήματα 5.8.14 και 5.8.16 τού U. Felger[96], στις αποδείξεις των οποίων υπεισέρχονται ειδικές παραγοντοποιήσεις στοιχείων τής Π.Μ.Π. $\mathfrak{O}_{-3} = \mathbb{Z}[\zeta_3]$.

5.8.14 Θεώρημα. *Έστω p ένας περιττός πρώτος αριθμός, τέτοιος ώστε να ισχύει $p \equiv 2(\mathrm{mod}\,3)$ και $p \not\equiv 8(\mathrm{mod}\,9)$. Ας υποθέσουμε ότι*

$$k = pa^3 - 3b^2,$$

όπου οι $a, b \in \mathbb{Z}$ ικανοποιούν τις ακόλουθες συνθήκες:

(i) $a \not\equiv 0(\mathrm{mod}\,p)$, $a \equiv 0(\mathrm{mod}\,3)$ *και* $a \equiv 1(\mathrm{mod}\,2)$.

(ii) $b \equiv 0(\mathrm{mod}\,p)$ *και* $b \not\equiv 0(\mathrm{mod}\,3)$.

(iii) $q \not\equiv 1(\mathrm{mod}\,3)$ *για κάθε πρώτον αριθμό q με $q \mid a$.*

Τότε η εξίσωση (5.132) *με παράμετρο k δεν διαθέτει ακέραιες λύσεις.*

[96] U. Felger: *On Bachet's diophantine equation $x^3 = y^2 + k$*, Monatsh. Math. **98** (1984), 185-191.

5.8.15 Παράδειγμα. Η παράμετρος $k = -30$ συγκαταλέγεται σε αυτές που περιγράφονται στο θεώρημα 5.8.14. (Αρκεί να τεθεί $a = 9, p = 5$ και $b = 35$.)

5.8.16 Θεώρημα. *Έστω p ένας πρώτος αριθμός με $p \equiv 1 (\mathrm{mod}\, 3)$ και $p \not\equiv 1 (\mathrm{mod}\, 9)$. Ας υποθέσουμε ότι*

$$k = pa^3 - 3b^2,$$

όπου οι $a, b \in \mathbb{Z}$ ικανοποιούν τις ακόλουθες συνθήκες:

(i) $a \not\equiv 0 (\mathrm{mod}\, p)$, $a \equiv 0 (\mathrm{mod}\, 3)$ *και* $a \equiv 1 (\mathrm{mod}\, 2)$.

(ii) $b \equiv 0 (\mathrm{mod}\, p)$ *και* $b \not\equiv 0 (\mathrm{mod}\, 3)$.

(iii) $q \not\equiv 1 (\mathrm{mod}\, 3)$ *για κάθε πρώτον αριθμό q με $q \mid a$.*

(iv) *Κάθε πρώτος αριθμός q με $q \mid b$ είναι ένας κύβος* $(\mathrm{mod}\, p)$.

Τότε η εξίσωση (5.132) *με παράμετρο k δεν διαθέτει ακέραιες λύσεις.*

5.8.17 Παράδειγμα. Η παράμετρος $k = 42$ συγκαταλέγεται σε αυτές που περιγράφονται στο θεώρημα 5.8.16. (Αρκεί να τεθεί $b = p = 2$ και $a = 3$.)

► **Υπολογισμοί λύσεων μέσω άνω φραγμάτων.** Όταν, αυξανομένης τής απόλυτης τιμής $|k|$ τής παραμέτρου k, τα όποια τεχνάσματα και οι λοιπές διαθέσιμες αλγεβρικές ή γεωμετρικές μέθοδοι δεν επαρκούν πλήρως, τότε, για τον *υπολογισμό* των ακεραίων λύσεων τής εξισώσεως (5.132) τού Mordell (ακόμη και για *αρκετά μεγάλες τιμές* τής $|k|$), προσφεύγουμε *εκ παραλλήλου* και σε πιο «δραστικά» τεχνικά μέσα, όπως είναι η εύρεση *άνω φραγμάτων* των $|x|, |y|$ μέσω κατάλληλων συναρτήσεων εξαρτώμενων από την παράμετρο k. Επί παραδείγματι, μέσω τού άνω φράγματος

$$\boxed{\max\{|x|, |y|\} \leq \exp(10^{10} |k|^{10^4}),}$$

τού A. Baker[97] ή μέσω τής προδήλως καλύτερης προσεγγίσεως[98]

$$\boxed{\max\{|x|, |y|\} \leq \exp(c\, |k|\, (1 + \ln(|k|))^6),}$$

όπου το c συμβολίζει κάποια απόλυτη (και υπολογιστέα) σταθερά, είναι δυνατόν (με τη βοήθεια των σύγχρονων ηλεκτρονικών υπολογιστών) να προσδιορισθεί το σύνολο των ακεραίων λύσεων τής (5.132) όταν[99] $|k| \leq 10^4$ (ή και για ακόμη μεγαλύτερες τιμές).

[97] A. Baker: *On the representation of integers of binary forms*, Philos. Trans. A **263** (1968), 173-208.

[98] Βλ. V.G. Sprindzuk: *Classical Diophantine Equations*, Lecture Notes in Math. **1559**, Springer-Verlag, 1993, Thm. 1.1, p. 113.

[99] Πρβλ. J. Gebel, A. Pethö & H. G. Zimmer: *On Mordell's equation*, Compositio Math. **110** (1998), 335-367.

► **Εξίσωση των Ramanujan και Nagell.** Αυτή αποτελεί άλλο ένα χαρακτηριστικό παράδειγμα τού πόσο χρήσιμο μπορεί να αποβεί το να έχουμε στη διάθεσή μας την ιδιότητα τής μονοσήμαντης παραγοντοποιήσεως εντός δοθείσας ακεραίας περιοχής.

5.8.18 Ορισμός. Η διοφαντική εξίσωση

$$\boxed{x^2+7=2^n,} \tag{5.152}$$

όπου $n\in\mathbb{N}$, καλείται **εξίσωση των Ramanujan και Nagell**.,

Το ότι η (5.152) διαθέτει ακέραιες λύσεις μόνον όταν $n\in\{3,4,5,7,15\}$ είχε διατυπωθεί ως εικασία από τον Srinivasa Ramanujan[100] (1887-1920) και (ανεξαρτήτως αυτού) από τον Wilhelm Ljunggren[101] (1905-1973). Η απόδειξη τού θεωρήματος 5.8.20 οφείλεται στον Trygve Nagell[102] (1895-1988). Σε αυτήν[103] (λαμβανομένου υπ' όψιν ότι ισχύει $-7\equiv 1(\mathrm{mod}\,4)$) χρησιμοποιείται ουσιωδώς το ότι ο δακτύλιος $\mathfrak{O}_{-7}\underset{5.5.2}{=}\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ των ακεραίων τού $\mathbb{Q}(\sqrt{-7})$, όντας **N**-ευκλείδεια περιοχή (κατά το θεώρημα 5.5.7), είναι Π.Μ.Π. (Βλ. θεώρημα 5.4.21 και πόρισμα 5.6.8.)

5.8.19 Λήμμα. *Εάν ένας $r\in\mathbb{N}$ γράφεται υπό τη μορφή $r=7^l s$, όπου $s,l\in\mathbb{N}$ και $7\nmid s$, τότε εντός τής Π.Μ.Π. $\mathfrak{O}_{-7}$ ισχύει η ισοτιμία*[104]

$$(1+\sqrt{-7})^r\equiv 1+r\sqrt{-7}(\mathrm{mod}\,7^{l+1}). \tag{5.153}$$

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς θα αποδείξουμε επαγωγικώς ότι για κάθε $j\in\mathbb{N}$ ισχύει η

$$(1+\sqrt{-7})^{7^j}\equiv 1+7^j\sqrt{-7}(\mathrm{mod}\,7^{j+1}). \tag{5.154}$$

Επειδή το 7 διαιρεί τον διωνυμικό συντελεστή $\binom{7}{\nu}$ για κάθε $\nu\in\{1,...,6\}$ και

$$(\sqrt{-7})^\nu=\begin{cases}(-7)^{\frac{\nu}{2}}, & \text{όταν } \nu\in\{2,4,6\},\\ (-7)^{\frac{\nu-1}{2}}(\sqrt{-7}), & \text{όταν } \nu\in\{3,5,7\}.\end{cases}$$

είναι προφανές ότι

$$\left\{\begin{array}{l}\binom{7}{\nu}\equiv 0(\mathrm{mod}\,7) \text{ και}\\ (\sqrt{-7})^\nu\equiv 0(\mathrm{mod}\,7),\\ \\ \forall\nu\in\{2,3,4,5,6\}\end{array}\right\}\Rightarrow\left\{\begin{array}{l}\binom{7}{\nu}(\sqrt{-7})^\nu\equiv 0(\mathrm{mod}\,7^2),\\ \\ \forall\nu\in\{2,3,4,5,6\}\end{array}\right\}$$

[100] S. Ramanujan: *Question* 464, J. Indian Math. Soc. **5** (1913), p. 130.

[101] W. Ljunggren: *Oppgave nr* 2, Norsk Mat. Tidsskr. **25** (1943), p. 29.

[102] Βλ. T. Nagell: *Losning till oppgave nr* 2, Norsk Mat. Tidsskr. **30** (1948), 62-64 και

T. Nagell: *The Diophantine equation* $x^2+7=2^n$, Ark. Mat. **4** (1961), 185-187.

[103] Η απόδειξη που παρατίθεται κατωτέρω χρησιμοποιεί την εργασία τού Nagell, τη σχετική εργασία τού
H. Hasse: *Über eine diophantische Gleichung von Ramanujan-Nagell und ihre Verallgemeinerung*, Nagoya Math. J. **27** (1966), 77-102, καθώς και κάποιους αναλυτικότερους υπολογισμούς.

[104] Στο λήμμα 5.8.19 και στην απόδειξη τού θεωρήματος 5.8.20 το σύμβολο "$\equiv$" τής ισοτιμίας νοείται *εντός τής* $\mathfrak{O}_{-7}$. (Γράφοντας $\alpha\equiv\beta(\mathrm{mod}\,\gamma)$ για κάποια $\alpha,\beta,\gamma\in\mathfrak{O}_{-7}$, εννοούμε ότι υπάρχει $\delta\in\mathfrak{O}_{-7}$, τέτοιο ώστε να ισχύει $a-\beta=\gamma\delta$. Φυσικά, αν τύχει και τα στοιχεία α,β,γ είναι ακέραιοι, τότε και το δ είναι κατ' ανάγκην ακέραιος.)

και $(\sqrt{-7})^7 = (-7)^3(\sqrt{-7}) \Rightarrow (\sqrt{-7})^7 \equiv 0(\mathrm{mod}\, 7^2)$, οπότε

$$(1+\sqrt{-7})^7 = \sum_{\nu=0}^{7} \tbinom{7}{\nu}(\sqrt{-7})^\nu \equiv 1 + 7\sqrt{-7}(\mathrm{mod}\, 7^2)$$

και η (5.154) είναι αληθής για $j = 1$. Υποθέτοντας ότι είναι αληθής για κάποιον $j \geq 1$, ήτοι ότι

$$\exists\, z \in \mathfrak{O}_{-7} : (1+\sqrt{-7})^{7^j} - 1 - 7^j\sqrt{-7} = 7^{j+1}z,$$

θα αποδείξουμε ότι είναι αληθής και για τον $j+1$. Προφανώς,

$$\begin{aligned}(1+\sqrt{-7})^{7^{j+1}} &= [(1+\sqrt{-7})^{7^j}]^7 = (1+7^j\sqrt{-7}+7^{j+1}z)^7 \\ &= (1+7^j\sqrt{-7})^7 + \underbrace{\sum_{\nu=1}^{7}\binom{7}{\nu}(7^{j+1}z)^\nu(1+7^j\sqrt{-7})^{7-\nu}}_{\equiv 0(\mathrm{mod}\, 7^{j+2})} \equiv (1+7^j\sqrt{-7})^7\,(\mathrm{mod}\, 7^{j+2})\end{aligned}$$

και

$$(1+7^j\sqrt{-7})^7 = \sum_{\nu=0}^{7}\tbinom{7}{\nu}(7^j\sqrt{-7})^\nu = 1 + 7^{j+1}\sqrt{-7} + \underbrace{\sum_{\nu=2}^{7}\tbinom{7}{\nu}(7^j\sqrt{-7})^\nu}_{\equiv 0(\mathrm{mod}\, 7^{j+2})},$$

οπότε $(1+\sqrt{-7})^{7^{j+1}} \equiv 1+7^{j+1}\sqrt{-7}(\mathrm{mod}\, 7^{j+2})$. Εν συνεχεία, υψώνοντας το άθροισμα $1+\sqrt{-7}$ στη δύναμη $r = 7^l s$ λαμβάνουμε

$$(1+\sqrt{-7})^r = [(1+\sqrt{-7})^{7^l}]^s \underset{(5.154)}{\equiv} (1+7^l\sqrt{-7})^s\,(\mathrm{mod}\, 7^{l+1}).$$

Επειδή

$$\begin{aligned}(1+7^l\sqrt{-7})^s &= \sum_{\nu=0}^{s}\tbinom{s}{\nu}(7^l\sqrt{-7})^\nu \\ &= 1 + 7^l s\sqrt{-7} + \underbrace{\sum_{\nu=2}^{s}\binom{s}{\nu}(7^l\sqrt{-7})^\nu}_{\equiv 0(\mathrm{mod}\, 7^{l+1})} \equiv 1 + r\sqrt{-7}(\mathrm{mod}\, 7^{l+1}),\end{aligned}$$

η (5.153) είναι ωσαύτως αληθής. □

5.8.20 Θεώρημα. *Οι μόνες λύσεις* $(x,n) \in \mathbb{Z}\times\mathbb{N}$ *της εξισώσεως* (5.152) *των Ramanujan και Nagell είναι οι*

$$(x,n) \in \{(\pm 1,3),(\pm 3,4),(\pm 5,5),(\pm 11,7),(\pm 181,15)\}.$$

ΑΠΟΔΕΙΞΗ. *Περίπτωση πρώτη.* Εάν ο n είναι άρτιος, τότε

$$(2^{\frac{n}{2}})^2 - x^2 = (2^{\frac{n}{2}} - x)(2^{\frac{n}{2}} + x) = 7,$$

οπότε το θεμελιώδες θεώρημα τής Αριθμητικής δίδει

$$(2^{\frac{n}{2}} - x, 2^{\frac{n}{2}} + x) \in \{(1,7),(7,1),(-1,-7),(-7,-1)\}$$
$$\Rightarrow (2^{\frac{n}{2}} - x) + (2^{\frac{n}{2}} + x) = 2^{\frac{n+2}{2}} \in \{\pm 8\} \Rightarrow 2^{\frac{n+2}{2}} = 8 \Rightarrow (x,n) = (\pm 3, 4).$$

Περίπτωση δεύτερη. Για $n = 1$ η (5.152) δεν διαθέτει (πραγματικές, πόσω δε μάλλον ακέραιες) λύσεις, διότι $x^2 \geq 0$, ενώ για $n = 3$ ο μόνοι ακέραιοι που την ικανοποιούν είναι οι -1 και 1, οπότε $(x,n) = (\pm 1, 3)$.

Περίπτωση τρίτη. Εάν ο n είναι περιττός ≥ 5, τότε ο $m := n - 2$ είναι περιττός ≥ 3 και η (5.152) γράφεται υπό τη μορφή

$$\frac{x^2 + 7}{4} = 2^m. \tag{5.155}$$

Θέτοντας $\alpha := \frac{1}{2}(1 + \sqrt{-7})$ και $\beta := \overline{\alpha} = \frac{1}{2}(1 - \sqrt{-7})$ παρατηρούμε ότι

$$\alpha + \beta = 1,\ \alpha - \beta = \sqrt{-7},\ \mathbf{N}(\alpha) = \mathbf{N}(\beta) = \alpha\beta = 2. \tag{5.156}$$

Εντός τής Π.Μ.Π. $\mathfrak{O}_{-7}$ η (5.155) εκφράζεται ως ακολούθως:

$$\left(\tfrac{x+\sqrt{-7}}{2}\right)\left(\tfrac{x-\sqrt{-7}}{2}\right) = 2^m = (\alpha\beta)^m = \alpha^m\beta^m. \tag{5.157}$$

Σημειωτέον ότι[105] $\mathbf{N}(\frac{x+\sqrt{-7}}{2}) = \mathbf{N}(\frac{x-\sqrt{-7}}{2}) = \frac{x^2+7}{4}$ και

$$\tfrac{x+\sqrt{-7}}{2} + \tfrac{x-\sqrt{-7}}{2} = x,\ \tfrac{x+\sqrt{-7}}{2} - \tfrac{x-\sqrt{-7}}{2} = \sqrt{-7}. \tag{5.158}$$

Ισχυρισμός πρώτος. Αμφότεροι οι μιγαδικοί αριθμοί α και β είναι *ανάγωγα στοιχεία* τής $\mathfrak{O}_{-7}$. Πράγματι· εάν $\alpha = \alpha_1\alpha_2$ για κάποια $\alpha_1, \alpha_2 \in \mathfrak{O}_{-7}$, τότε

$$\left\{\begin{array}{l} 2 = \mathbf{N}(\alpha) = \mathbf{N}(\alpha_1)\mathbf{N}(\alpha_2) \\ \mathbf{N}(\alpha_1), \mathbf{N}(\alpha_2) \in \mathbb{N}_0 \text{ (βλ. (5.51))} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \text{είτε } \ (\mathbf{N}(\alpha_1), \mathbf{N}(\alpha_2)) = (1,2) \\ \text{είτε } \ (\mathbf{N}(\alpha_1), \mathbf{N}(\alpha_2)) = (2,1) \end{array}\right\}.$$

Επειδή είτε $\alpha_1 \in \mathfrak{O}_{-7}^{\times}$ $(= \{\pm 1\})$ είτε $\alpha_2 \in \mathfrak{O}_{-7}^{\times}$, τούτο σημαίνει ότι ο α είναι ανάγωγο στοιχείο τής $\mathfrak{O}_{-7}$. (Βλ. 5.5.3 (iii) και 5.2.39 (vi).) Η απόδειξη τού ότι *και* ο β είναι ανάγωγο στοιχείο τής $\mathfrak{O}_{-7}$ είναι πανομοιότυπη.

Ισχυρισμός δεύτερος. Από την (5.157) έπεται ότι

$$(\tfrac{x+\sqrt{-7}}{2}, \tfrac{x-\sqrt{-7}}{2}) \in \{(\alpha^m, \beta^m), (-\alpha^m, \beta^m), (\alpha^m, -\beta^m), (-\alpha^m, -\beta^m)\}. \tag{5.159}$$

[105] Για την εύρεση τής τιμής τής αριθμητικής στάθμης $\mathbf{N}$ σε ένα στοιχείο τής $\mathfrak{O}_{-7}$ βλ. το (i) τού εδαφίου 5.5.3.

Έστω $d \in \text{ΜΚΔ}_{\mathfrak{O}_{-7}}(\frac{x+\sqrt{-7}}{2}, \frac{x-\sqrt{-7}}{2})$. Λόγω των (5.158) η αριθμητική στάθμη $\mathbf{N}(d)$ τού d οφείλει να πληροί τις συνθήκες:

$$\left\{ \begin{array}{l} d \mid x \\ d \mid \sqrt{-7} \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} \mathbf{N}(d) \mid \mathbf{N}(x) = x^2 \\ \mathbf{N}(d) \mid \mathbf{N}(\sqrt{-7}) = 7 \end{array} \right\} \Rightarrow \mathbf{N}(d) \mid x^2 + 7 = 2^{m+2} \qquad (5.160)$$

και

$$d \mid \sqrt{-7} \Rightarrow \left\{ \begin{array}{l} \mathbf{N}(d) \mid \mathbf{N}(\sqrt{-7}) = 7 \\ \mathbf{N}(d) \in \mathbb{N}_0 \text{ (βλ. (5.51))} \end{array} \right\} \Rightarrow \mathbf{N}(d) \in \{1, 7\}. \qquad (5.161)$$

Οι (5.160) και (5.161) δίδουν $\mathbf{N}(d) = 1$, απ' όπου έπεται ότι τα στοιχεία $\frac{x+\sqrt{-7}}{2}$ και $\frac{x-\sqrt{-7}}{2}$ είναι *πρώτα μεταξύ τους* εντός τής $\mathfrak{O}_{-7}$. Επειδή $1^m = 1$ και $(-1)^m = -1$, υφίστανται (σύμφωνα με το (ii) τού πορίσματος 5.6.15) $t, w \in \mathfrak{O}_{-7}^{\times} \setminus \{0, \pm 1\}$, ούτως ώστε να ισχύουν οι ισότητες

$$\tfrac{x+\sqrt{-7}}{2} = t^m \text{ και } \tfrac{x-\sqrt{-7}}{2} = w^m.$$

Επειδή αμφότεροι οι α και β διαιρούν το δεξιό μέλος τής (5.157) και είναι ανάγωγα (και, κατ' επέκταση, πρώτα) στοιχεία τής $\mathfrak{O}_{-7}$, καθένας εξ αυτών θα διαιρεί είτε τον $\frac{x+\sqrt{-7}}{2}$ είτε τον $\frac{x-\sqrt{-7}}{2}$. Ωστόσο, κανείς εξ αυτών δεν θα διαιρεί αμφότερους τους $\frac{x+\sqrt{-7}}{2}$ και $\frac{x-\sqrt{-7}}{2}$ (εντός τής $\mathfrak{O}_{-7}$). Πράγματι· εάν υποθέσουμε ότι ο α διαιρεί αμφότερους τους $\frac{x+\sqrt{-7}}{2}$ και $\frac{x-\sqrt{-7}}{2}$, τότε θα διαιρεί και τη διαφορά τους $\sqrt{-7}$ (βλ. (5.158)), και θα υπάρχει $z \in \mathfrak{O}_{-7}$, τέτοιος ώστε να ισχύει

$$\sqrt{-7} = \alpha z \Rightarrow 7 = \mathbf{N}(\sqrt{-7}) = \mathbf{N}(\alpha)\mathbf{N}(z) = 2 \underbrace{\mathbf{N}(z)}_{\in \mathbb{N}_0}.$$

Τούτο όμως είναι άτοπο, διότι το 7 είναι περιττός. (Η απόδειξη για το ότι *και* ο β έχει αυτήν την ιδιότητα είναι πανομοιότυπη.) Εάν ο α διαιρεί τον $\frac{x+\sqrt{-7}}{2} = t^m$, τότε ο α διαιρεί τον[106] t (διότι $\alpha \neq \pm 1$) και ο β (λόγω των προαναφερθέντων) διαιρεί τον $\frac{x-\sqrt{-7}}{2} = w^m$ και, ως εκ τούτου, τον w. Επομένως,

$$\exists\, (\gamma, \delta) \in \mathfrak{O}_{-7} \times \mathfrak{O}_{-7} : [t = \alpha\gamma \text{ και } w = \beta\delta]$$
$$\Rightarrow t^m w^m = (\gamma^m \delta^m)\, \alpha^m \beta^m = \alpha^m \beta^m \Rightarrow \gamma^m \delta^m = 1.$$

Εξ αυτού καταλήγουμε στο ότι $\gamma, \delta \in \mathfrak{O}_{-7}^{\times}$ $(= \{\pm 1\})$ και στο ίδιο συμπέρασμα εάν (στην ανωτέρω υπόθεσή μας) εναλλάξουμε τους ρόλους των α και β. Άρα ο ισχυρισμός είναι αληθής. Επιπροσθέτως, ασχέτως με το ποια εκ των τεσσάρων τιμών λαμβάνει το διατεταγμένο ζεύγος $(\frac{x+\sqrt{-7}}{2}, \frac{x-\sqrt{-7}}{2})$ στην (5.159), ισχύει

$$\pm\sqrt{-7} = \alpha^m - \beta^m. \qquad (5.162)$$

[106] Ο α (ως πρώτο στοιχείο τής $\mathfrak{O}_{-7}$) διαιρεί τον t.

Ισχυρισμός τρίτος. Το πρόσημο $+$ *δεν είναι δυνατόν να εμφανίζεται* στην (5.162). Πράγματι· εάν η (5.162) ήταν αληθής με το πρόσημο $+$, τότε θα είχαμε

$$\alpha^m - \beta^m = \sqrt{-7} \underset{(5.156)}{=} \alpha - \beta, \tag{5.163}$$

$\alpha^2 \underset{(5.156)}{=} (1-\beta)^2 = 1 + \beta^2 - \underbrace{2}_{=\alpha\beta}\beta = 1 + \beta^2 - \alpha\beta^2 \equiv 1 (\mathrm{mod}\, \beta^2)$ και, ως εκ τούτου,

$$m \geq 3 \Rightarrow \left\{ \begin{array}{l} \alpha^m = \alpha(\alpha^2)^{\frac{m-1}{2}} \equiv \alpha (\mathrm{mod}\, \beta^2) \\ \beta^m \equiv 0 (\mathrm{mod}\, \beta^2) \end{array} \right\} \Rightarrow \alpha^m - \beta^m \equiv \alpha (\mathrm{mod}\, \beta^2), \tag{5.164}$$

και από τις (5.163) και (5.164) θα έπετο ότι

$$\alpha - \beta \equiv \alpha (\mathrm{mod}\, \beta^2) \Rightarrow \beta \equiv 0 (\mathrm{mod}\, \beta^2) \Rightarrow 4 = \mathbf{N}(\beta^2) \mid \mathbf{N}(\beta) = 2.$$

Άτοπο! Επομένως,

$$-\sqrt{-7} = \alpha^m - \beta^m \Rightarrow -1 = \frac{\alpha^m - \beta^m}{\sqrt{-7}} = \frac{\left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1-\sqrt{-7}}{2}\right)^m}{\sqrt{-7}}. \tag{5.165}$$

Το διωνυμικό ανάπτυγμα τού δεξιού μέλους τής (5.165) δίδει

$$\frac{\sum_{j=0}^{m} \binom{m}{j} \left(\sqrt{-7}\right)^j - \sum_{j=0}^{m} \binom{m}{j} (-1)^j \left(\sqrt{-7}\right)^j}{2^m \sqrt{-7}}$$

$$= \frac{\sum_{j=0}^{m} (1-(-1)^j) \binom{m}{j} \left(\sqrt{-7}\right)^j}{2^m \sqrt{-7}} = \frac{\sum_{j=1}^{\frac{m+1}{2}} \binom{m}{2j-1} 7^{j-1}}{2^{m-1}}$$

και η (5.165) ισοδυναμεί με την

$$-2^{m-1} = \sum_{j=1}^{\frac{m+1}{2}} \binom{m}{2j-1} 7^{j-1} = m + 7 \left[\sum_{j=2}^{\frac{m+1}{2}} \binom{m}{2j-1} 7^{j-2} \right],$$

οπότε (εντός τού $\mathbb{Z}$!) ισχύει η ισοτιμία

$$-2^{m-1} \equiv m (\mathrm{mod}\, 7). \tag{5.166}$$

Επειδή ο $m-1$ είναι άρτιος, διαιρούμενος διά τού 6 αφήνει υπόλοιπο $0, 2$ ή 4.

(i) Εάν $m - 1 \equiv 0 (\mathrm{mod}\, 6)$, τότε $2^6 \equiv 1 (\mathrm{mod}\, 7) \Rightarrow 2^{m-1} = (2^6)^{\frac{m-1}{6}} \equiv 1 (\mathrm{mod}\, 7)$ και

$$m \underset{(5.166)}{\equiv} -2^{m-1} (\mathrm{mod}\, 7) \equiv -(2^6)^{\frac{m-1}{6}} (\mathrm{mod}\, 7) \equiv -1 (\mathrm{mod}\, 7) \equiv 6 (\mathrm{mod}\, 7).$$

Από το λήμμα 3.4.13 συνάγεται ότι[107]

$$\left\{\begin{array}{l} m \equiv 1(\mathrm{mod}\, 6) \\ m \equiv 6(\mathrm{mod}\, 7) \end{array}\right\} \Longrightarrow m \equiv 13(\mathrm{mod}\ 42).$$

(ii) Εάν $m-1 \equiv 2(\mathrm{mod}\, 6)$, τότε $2^6 \equiv 1(\mathrm{mod}\, 7) \Rightarrow 2^{m-3} = (2^6)^{\frac{m-3}{6}} \equiv 1(\mathrm{mod}\, 7)$ και

$$m \equiv -2^{m-1}(\mathrm{mod}\, 7) \equiv -2^2(2^6)^{\frac{m-3}{6}}(\mathrm{mod}\, 7) \equiv -4(\mathrm{mod}\, 7) \equiv 3(\mathrm{mod}\, 7).$$

Από το λήμμα 3.4.13 συνάγεται κατ' αναλογίαν ότι

$$\left\{\begin{array}{l} m \equiv 3(\mathrm{mod}\, 6) \\ m \equiv 3(\mathrm{mod}\, 7) \end{array}\right\} \Longrightarrow m \equiv 3(\mathrm{mod}\ 42).$$

(iii) Εάν $m-1 \equiv 4(\mathrm{mod}\, 6)$, τότε $2^6 \equiv 1(\mathrm{mod}\, 7) \Rightarrow 2^{m-5} = (2^6)^{\frac{m-5}{6}} \equiv 1(\mathrm{mod}\, 7)$ και

$$m \equiv -2^{m-1}(\mathrm{mod}\, 7) \equiv -2^4(2^6)^{\frac{m-5}{6}}(\mathrm{mod}\, 7) \equiv -16(\mathrm{mod}\, 7) \equiv 5(\mathrm{mod}\, 7).$$

Από το λήμμα 3.4.13 συνάγεται κατ' αναλογίαν ότι

$$\left\{\begin{array}{l} m \equiv 5(\mathrm{mod}\, 6) \\ m \equiv 5(\mathrm{mod}\, 7) \end{array}\right\} \Longrightarrow m \equiv 5(\mathrm{mod}\ 42).$$

Ισχυρισμός τέταρτος. Οι αριθμοί $3, 5$ και 13 είναι *οι μόνοι περιττοί ακέραιοι* $m \geq 3$ *που προέρχονται από την* (5.155) *και οι κλάσεις των οποίων εντός τού δακτυλίου* $\mathbb{Z}_{42}$ *ικανοποιούν την* (5.166). Έστω ότι m_1, m_2 είναι περιττοί ακέραιοι ≥ 3 με $[m_1]_{42} = [m_2]_{42}$ ικανοποιούντες την (5.166). Τότε έχουμε

$$\left\{\begin{array}{l} -m_1 \equiv 2^{m_1-1}(\mathrm{mod}\, 7) \\ -m_2 \equiv 2^{m_2-1}(\mathrm{mod}\, 7) \text{ και} \\ \\ m_2 \equiv m_1(\mathrm{mod}\, 42) \end{array}\right\}.$$

Για την επαλήθευση τού ισχυρισμού αρκεί να αποδείξουμε ότι $m_1 = m_2$. Θα χρησιμοποιήσουμε «εις άτοπον απαγωγή». Υποθέτουμε (δίχως βλάβη τής γενικότητας) ότι $m_2 > m_1$. Προφανώς, $m_2 - m_1 = 7^l \cdot 6 \cdot s$, για κάποιους $s, l \in \mathbb{N}$ με $7 \nmid s$. Επειδή

$$\alpha^{m_2} = \alpha^{m_1}\alpha^{m_2-m_1} = \alpha^{m_1}\tfrac{1}{2^{m_2-m_1}}(1+\sqrt{-7})^{m_2-m_1},$$

το λήμμα 5.8.19 μας πληροφορεί ότι

$$2^{m_2-m_1}\alpha^{m_2} = \alpha^{m_1}(1+\sqrt{-7})^{m_2-m_1} \equiv \alpha^{m_1} + (m_2-m_1)\alpha^{m_1}\sqrt{-7}(\mathrm{mod}\ 7^{l+1}). \quad (5.167)$$

[107] Επειδή μκδ$(6,7) = 1 = 6 \cdot 6 + (-5) \cdot 7$, μέσω των προαναφερθέντων στην απόδειξη τού λήμματος 3.4.13 λαμβάνουμε (κατόπιν αναγωγής) $m \equiv (1 + 30 \cdot 6) \equiv 181 \equiv 13(\mathrm{mod}\ 42)$.

Κατ' αναλογίαν,

$$2^{m_2-m_1}\beta^{m_2} = \beta^{m_1}(1-\sqrt{-7})^{m_2-m_1} \equiv \beta^{m_1} - (m_2-m_1)\beta^{m_1}\sqrt{-7} (\mathrm{mod}\ 7^{l+1}). \quad (5.168)$$

Κατόπιν κατά μέλη αφαιρέσεως τής (5.168) από την (5.167) λαμβάνουμε

$$2^{m_2-m_1}(\alpha^{m_2} - \beta^{m_2}) \equiv \alpha^{m_1} - \beta^{m_1} + (m_2-m_1)(\alpha^{m_1} + \beta^{m_1})\sqrt{-7} (\mathrm{mod}\ 7^{l+1}). \quad (5.169)$$

Επειδή

$$2^{m_2-m_1} = (2^6)^{\frac{m_2-m_1}{6}} = (1+9\cdot 7)^{7^l s} = 1 + \sum_{\nu=1}^{7^l s} \binom{7^l s}{\nu} (9\cdot 7)^{\nu}$$

και

$$\binom{7^l s}{\nu}(9\cdot 7)^{\nu} = 7^{l+\nu}\left[\tfrac{9^{\nu}}{\nu}\binom{7^l s-1}{\nu-1}\right] s \equiv 0 (\mathrm{mod}\, 7^{l+1}),\ \forall \nu \in \{1, ..., 7^l s\},$$

έχουμε

$$2^{m_2-m_1} \equiv 1 (\mathrm{mod}\ 7^{l+1}). \quad (5.170)$$

Επειδή δε, $\alpha^{m_2} - \beta^{m_2} = \alpha^{m_1} - \beta^{m_1} = -\sqrt{-7}$ (βλ. (5.165)), από τις (5.169) και (5.170) συνάγεται ότι

$$(m_2-m_1)(\alpha^{m_1} + \beta^{m_1})\sqrt{-7} \equiv 0 (\mathrm{mod}\ 7^{l+1}).$$

Άρα $\exists\,(\kappa,\xi) \in \mathbb{Z}\times\mathbb{Z} : 7^l\,(6s)\,(\alpha^{m_1}+\beta^{m_1})\sqrt{-7} = 7^{l+1}(\kappa+\xi\alpha)$, απ' όπου έπεται ότι

$$6s(\alpha^{m_1}+\beta^{m_1}) = -\sqrt{-7}\left(\kappa + \tfrac{1+\sqrt{-7}}{2}\xi\right) = \tfrac{7}{2}\xi - (\kappa+\tfrac{\xi}{2})\sqrt{-7}. \quad (5.171)$$

Χρησιμοποιώντας τόν τύπο[108]

$$\begin{aligned}\alpha^{m_1}+\beta^{m_1} &= \sum_{j=0}^{\frac{m_1-1}{2}} (-1)^j \underbrace{\tfrac{m_1}{m_1-j}\binom{m_1-j}{j}}_{\in\mathbb{Z}} 2^j = \sum_{j=0}^{\frac{m_1-1}{2}} (-1)^j \tfrac{(m_1-j-1)!m_1}{(m_1-2j)!j!}2^j \\ &= 1 - 2m_1(1 - \tfrac{(m_1-3)}{2}2 + \tfrac{(m_1-4)(m_1-5)}{6}2^2 - \cdots) \in \mathbb{Z}\end{aligned}$$

η (5.171) δίδει $\kappa = -\frac{\xi}{2} \Rightarrow 6s(\alpha^{m_1}+\beta^{m_1}) = -7\kappa$ και (επειδή $7 \nmid 6$ και $7 \nmid s$) το 7 οφείλει (εντός τού $\mathbb{Z}$!) να διαιρεί τον περιττό ακέραιο αριθμό $\alpha^{m_1}+\beta^{m_1}$, οπότε

[108] Για οιουσδήποτε $z, w \in \mathbb{C}$ και $m \in \mathbb{N}$ ισχύει *ο τύπος τού Waring*:

$$z^m + w^m = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} (-1)^j \tfrac{m}{m-j}\binom{m-j}{j}(z+w)^{m-2j}(zw)^j.$$

$\exists \varrho \in \mathbb{Z} : \alpha^{m_1} + \beta^{m_1} = 7\varrho$. Από την άλλη μεριά, το σύνηθες διωνυμικό ανάπτυγμα δίδει

$$\begin{aligned}
\alpha^{m_1} + \beta^{m_1} &= \left(\tfrac{1+\sqrt{-7}}{2}\right)^{m_1} + \left(\tfrac{1-\sqrt{-7}}{2}\right)^{m_1} \\
&= \tfrac{1}{2^{m_1}} \left[\sum_{j=0}^{m_1} \binom{m_1}{j} \left(\sqrt{-7}\right)^j + \sum_{j=0}^{m_1} \binom{m_1}{j} (-1)^j \left(\sqrt{-7}\right)^j \right] \\
&= \tfrac{1}{2^{m_1}} \left[\sum_{j=0}^{m_1} (1 + (-1)^j) \binom{m_1}{j} \left(\sqrt{-7}\right)^j \right] \\
&= \tfrac{1}{2^{m_1-1}} \left[\binom{m_1}{0} + \binom{m_1}{2} (-7) + \binom{m_1}{4} (-7)^2 + \cdots + \binom{m_1}{m_1-1} (-7)^{\frac{m_1-1}{2}} \right] \\
&= \tfrac{1}{2^{m_1-1}} (1 - 7\lambda),
\end{aligned}$$

όπου $\lambda := \binom{m_1}{2} + \binom{m_1}{4} (-7) + \binom{m_1}{6} (-7)^2 + \cdots + \binom{m_1}{m_1-1} (-7)^{\frac{m_1-3}{2}} \in \mathbb{Z}$, απ' όπου έπεται ότι

$$7\varrho = \tfrac{1}{2^{m_1-1}} (1 - 7\lambda) \Rightarrow 1 = 7(2^{m_1-1}\varrho + \lambda).$$

Άτοπο! Άρα έχουμε κατ' ανάγκην $m_1 = m_2$.

Αποπεράτωση αποδείξεως. Επειδή οι αριθμοί $3, 5$ και 13 είναι οι μόνοι περιττοί ακέραιοι m με $3 \leq m := n - 2 < 42$ που προέρχονται από την (5.155) και ικανοποιούν την (5.166), οι μόνες (υπολειπόμενες) λύσεις τής εξισώσεως (5.152) των Ramanujan και Nagell (που υπάγονται στην παρούσα τρίτη περίπτωση) είναι (κατά τα προαναφερθέντα) αυτές τού καταλόγου:

m	3	5	13
n	5	7	15
x	± 5	± 11	± 181

καθώς έχουμε $x = \pm\sqrt{2^n - 7}$. □

5.8.21 Σημείωση. Η διοφαντική εξίσωση

$$\boxed{x^2 - D = p^n,} \tag{5.172}$$

όπου $n \in \mathbb{N}$, p ένας πρώτος αριθμός και D ένας αρνητικός ακέραιος αριθμός, καλείται **γενικευμένη εξίσωση των Ramanujan και Nagell**. (Στο θεώρημα 5.8.20 πραγματευθήκαμε μόνον την περίπτωση κατά την οποία $D = -7$ και $p = 2$.) Για *περιττούς* πρώτους αριθμούς p αποδεικύονται (μέσω τής λεγομένης *μεθόδου των Lucas και Lehmer*) τα ακόλουθα[109]:

[109] Βλ. R.A. Mollin: *Advanced Number Theory with Applications*, CRC Press, 2010, Theorems 8.2 and 8.3, pp. 276-280.

(i) Εάν $p \geq 3$, $D \equiv 5 (\mathrm{mod}\, 8)$ και $d := \min\{ k \in \mathbb{N} |\, a^2 - Db^2 = 4p^k \}$, για κάποιους $a, b \in \mathbb{N}$ με μκδ$(bD, 2p) = 1$ και $(D, p) \neq (-3, 7)$, τότε η (5.172) διαθέτει λύσεις $(x, n) \in \mathbb{Z} \times \mathbb{N}$ εάν και μόνον εάν $b = 1$ και $D = -3a^2 \pm 8$. Εν τοιαύτη περιπτώσει,

$$(x, n) \in \left\{ (-\tfrac{a(a^2+3D)}{8}, 3d), (\tfrac{a(a^2+3D)}{8}, 3d) \right\}.$$

(ii) Εάν $p \geq 3$, $p \nmid D$ και $d := \min\{ k \in \mathbb{N} |\, a^2 - Db^2 = p^k \}$, για κάποιους $a, b \in \mathbb{N}$, τότε η (5.172) διαθέτει λύσεις $(x, n) \in \mathbb{Z} \times \mathbb{N}$ με $n > d$ εάν και μόνον εάν $b = 1$ και $n = dq$, όπου q κάποιος περιττός πρώτος αριθμός. Ιδιαιτέρως, εάν $3 \mid n$, τότε εν τοιαύτη περιπτώσει, $d = 1,\ D = -3a^2 \pm 1$,

$$p = 4a^2 \pm 1 \text{ και } (x, n) \in \left\{ (8a^3 \pm 3a, 3), (-(8a^3 \pm 3a), 3) \right\}.$$

5.8.22 Παραδείγματα. (i) Οι μόνες λύσεις $(x, n) \in \mathbb{Z} \times \mathbb{N}$ τής $x^2 + 19 = 7^n$ (με $D = -19$, $a = 3$, $b = 1$, $d = 1$) είναι οι

$$(x, n) \in \{ (18, 3), (-18, 3) \}.$$

(ii) Οι μόνες λύσεις $(x, n) \in \mathbb{Z} \times \mathbb{N}$ τής $x^2 + 2 = 3^n$ όταν $3 \mid n$ (με $D = -2$, $a = b = d = 1$) είναι οι

$$(x, n) \in \{ (5, 3), (-5, 3) \}.$$

(iii) Η $x^2 + 5 = 41^n$, όπου $3 \mid n$, δεν διαθέτει καμία λύση $(x, n) \in \mathbb{Z} \times \mathbb{N}$, διότι $6^2 + 5 = 41$ (όπου $a = 6$, $b = 1$, $d = 1$) αλλά $D = -5 \neq -3 \cdot 6^2 \pm 1$.