Κεφαλαιο 1

Διαιρετοτητα και Πρωτοι Αριθμοι

Η ανάπτυξη της Θεωρίας Αριθμών πηγάζει από τη προσπάθεια του ανθρώπου να κατανοήσει τις σχέσεις μεταξύ των ακεραίων αριθμών που προκύπτουν όταν τους προσθέτουμε και τους πολλαπλασιάζουμε.

Στο κεφάλαιο αυτό ο σκοπός μας είναι να μελετήσουμε λεπτομερώς ορισμένες από τις βασικές ιδιότητες των ακεραίων αριθμών που απορρέουν κυρίως από τον πολλαπλασιασμό τους.

1.1 Μαθηματική Επαγωγή

Θεωρούμε τα σύνολα των φυσικών αριθμών και των ακεραίων αριθμών που τα συμβολίζουμε αντίστοιχα με

$$\mathbb{N} = \{0, 1, 2, \ldots\} \quad \text{και}$$
$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}.$$

Επίσης τα σύνολα των ρητών των πραγματικών και των μιγαδικών αριθμών θα τα συμβολίζουμε αντίστοιχα με $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$.

Τους φυσικούς αριθμούς τους χρησιμοποιούμε από τότε που μαθαίνουμε να μετράμε. Η Θεωρία Συνόλων εγγυάται την ύπαρξη και την αυστηρή θεμελίωσή τους που αυτή γίνεται μέσω των αξιωμάτων του Peano.

Από τα αξιώματα αυτά ορίζονται οι πράξεις της πρόσθεσης και του πολλαπλασιασμού όπως επίσης και η διάταξη των ακεραίων αριθμών $\cdots < -1 < 0 < 1 < \cdots$.

Δεν θα αναφερθούμε διεξοδικά στα θέματα αυτά, στα οποία ο αναγνώστης μπορεί να ανατρέξει σε πολλά από τα εγχειρίδια της Θεωρίας Συνόλων και Λογικής. Εδώ παίρνουμε ως δεδομένο ότι είμαστε εξοικειωμένοι απ' τα μαθητικά μας χρόνια με τις πλέον βασικές ιδιότητες της πρόσθεσης και του πολλαπλασιασμού.

Στη Θεωρία Αριθμών αλλά και σε όλους τους κλάδους των Μαθηματικών, μία από τις αποδεικτικές μεθόδους είναι η Αρχή της Μαθηματικής Επαγωγής που αποτελεί ένα από τα αξιώματα του Peano. Υπάρχουν διάφορες ισοδύναμες μορφές διατύπωσης αυτής της αρχής που η κάθε μία απ' αυτές μας δίνει το κατάλληλο τρόπο εφαρμογής της για την απόδειξη ενός συγκεκριμένου προβλήματος. Θεωρούμε σκόπιμο εδώ να αναφέρουμε ορισμένες απ' αυτές τις μορφές και να αποδείξουμε την ισοδυναμία τους. Επιπλέον, παραθέτουμε μερικά χαρακτηριστικά παραδείγματα από τα οποία υποδεικνύεται ο τρόπος εφαρμογής αυτών των μορφών.

1.1.1 Πρόταση. ***Αρχή της Μαθηματικής Επαγωγής (ΑΜΕ).***

Έστω S ένα υποσύνολο των φυσικών αριθμών που έχει τις εξής δύο ιδιότητες.

(1) $0 \in S$.

(2) Αν $s \in S$ *έπεται ότι και* $s+1 \in S$.

Τότε $S = \mathbb{N}$.

1.1.2 Πρόταση. ***Αρχή της Πλήρους Μαθηματικής Επαγωγής.***

Έστω S ένα υποσύνολο των φυσικών αριθμών που έχει τις εξής δυο ιδιότητες.

(3) $0 \in S$.

(4) Αν $0, 1, 2, \ldots, s \in S$ *έπεται ότι και* $s+1 \in S$.

Τότε $S = \mathbb{N}$.

1.1.3 Πρόταση. ***Αρχή του Ελαχίστου.***

Κάθε μη κενό υποσύνολο S των φυσικών αριθμών έχει ελάχιστο στοιχείο, δηλαδή υπάρχει $s_0 \in S$ *με την ιδιότητα* $s \geq s_0$, *για κάθε* $s \in S$.

1.1.4 Πρόταση. ***Αρχή της Άπειρης Καθόδου.***

Δεν υπάρχει άπειρη γνήσια φθίνουσα ακολουθία φυσικών αριθμών.

1.1.5 Θεώρημα. *Οι Προτάσεις 1.1.1 έως 1.1.4 είναι όλες ισοδύναμες.*

Απόδειξη. 1.1.1 $\Rightarrow$ 1.1.2. Θεωρούμε το σύνολο S στο 1.1.2 και το σύνολο $T = \{n \in \mathbb{N}/0, 1, 2, \ldots, n \in S\}$.

Αφού $0 \in S$ έπεται ότι $0 \in T$. Αν $t \in T$, δηλαδή αν $0, 1, 2, \ldots, t \in S$, έπεται ότι $t + 1 \in S$. Οπότε $t + 1 \in T$. Λόγω της 1.1.1, πρέπει $T = \mathbb{N}$ και συνεπώς και $S = \mathbb{N}$.

1.1.2 $\Rightarrow$ 1.1.1. Θεωρούμε το σύνολο S στο 1.1.1. Αν $k \in S$ τότε $k+1 \in S$. Επειδή $0 \in S$ έπεται $1 \in S$ έπεται $2 \in S, \ldots$, έπεται ότι $k+1 \in S$. Δηλαδή αν $0, 1, \ldots, k \in S$ έπεται ότι $k + 1 \in S$. Συνεπώς από το 1.1.2, $S = \mathbb{N}$.

1.1.1 $\Rightarrow$ 1.1.3. Έστω S ένα μη κενό υποσύνολο των φυσικών αριθμών. Αν $0 \notin S$, θεωρούμε το σύνολο $T = \{n \in \mathbb{N}/$κανένα από τα στοιχεία $0, 1, 2, \ldots, n$ δεν ανήκουν στο $S\}$. Αν υπάρχει $k \in T$ με $k + 1 \notin T$, τότε το $k + 1$ είναι το ελάχιστο στοιχείο του S. Διαφορετικά, αν για όλα τα $k \in T$ το $k + 1 \in T$, τότε από το 1.1.1 έπεται ότι $T = \mathbb{N}$ και άρα $S = \emptyset$.

1.1.3 $\Rightarrow$ 1.1.1. Έστω S ένα σύνολο που ικανοποιεί τις ιδιότητες (1) και (2) στο 1.1.1. Υποθέτουμε ότι $S \neq \mathbb{N}$, οπότε το συμπλήρωμα του $S' \neq \emptyset$. Άρα το S' έχει ελάχιστο στοιχείο m. Απ' την ιδιότητα (1) πρέπει $m > 0$. Επειδή το m είναι ελάχιστο στοιχείο του S' το $m - 1 \notin S'$, δηλαδή $m - 1 \in S$. Αλλά τότε, απ' την ιδιότητα (2) του 1.1.1, έπεται ότι το $m \in S$, που είναι άτοπο. Άρα πρέπει $S' = \emptyset$, δηλαδή $S = \mathbb{N}$.

1.1.3 $\Rightarrow$ 1.1.4. Έστω $\alpha_1 > \alpha_2 > \cdots > \alpha_k > \alpha_{k+1} > \ldots$ μια άπειρη γνήσια φθίνουσα ακολουθία φυσικών αριθμών. Θεωρούμε το σύνολο $S = \{\alpha_s/s \in \mathbb{N}\}$. Το S έχει ελάχιστο στοιχειο, έστω α_{s_0}, για κάποιο $s_0 \in \mathbb{N}$. Αλλά $\alpha_{s_0} > \alpha_{s_0+1}$, δηλαδή $\alpha_{s_0+1} \in S$, που είναι άτοπο. Συνεπώς δεν μπορεί να υπάρχει τέτοια ακολουθία φυσικών αριθμών.

1.1.4 $\Rightarrow$ 1.1.3. Έστω S ένα μη κενό υποσύνολο των φυσικών αριθμών. Αν $k \in S$ δεν είναι ελάχιστο, τότε υπάρχει ένα $k' \in S$ με $k' < k$. Αν k' δεν είναι ελάχιστο υπάρχει $k' \in S$, $k'' < k'$. Συνεχίζοντας μ' αυτό τον

τρόπο κατασκευάζουμε μία γνήσια φθίνουσα ακολουθία που πρέπει να σταματά. □

Μία ισοδύναμη διατύπωση της 1ης και της 2ης μορφής της ΑΜΕ, που συνήθως χρησιμοποιείται στις εφαρμογές, αναφέρεται σε προτάσεις που αφορούν φυσικούς αριθμούς παρά σε σύνολα φυσικών αριθμών. Για παράδειγμα, η ισοδύναμη διατύπωση για την 1η μορφή έχει ως εξής:

Έστω $P(n)$ μια πρόταση που αφορά φυσικούς αριθμούς n. Αν για την $P(n)$ ισχύουν

(1) η $P(0)$ αληθεύει

(2) αν η $P(n)$ αληθεύει, έπεται ότι και η $P(n+1)$ αληθεύει. Τότε η $P(n)$ αληθεύει για κάθε φυσικό αριθμό.

Η ισχύς αυτής της διατύπωσης είναι προφανής αν θέσουμε στην 1.1.1 ως S το σύνολο $S = \{n \in \mathbb{N}/P(n) \text{ αληθεύει}\}$, οπότε $s \in S$, αν και μόνον αν η $P(s)$ αληθεύει.

Επίσης την 1η και 2η μορφή της ΑΜΕ μπορούμε να την εφαρμόζουμε με την εξής μικρή τροποποίηση:

Αν το $S' \subseteq \{n \in \mathbb{N}/n \geq n_0\}$, $n_0 \in \mathbb{N}$, έχει τις ιδιότητες

(1) $n_0 \in S'$

(2) αν $s \in S'$, έπεται ότι και $s+1 \in S'$

$$\left(\begin{array}{l}\text{ή}\\ \text{(4) αν } \ n_0, n_0+1, \ldots, s \in S' \ \text{ έπεται ότι και } \ s+1 \in S'.\end{array}\right)$$

Τότε $S' = \{n \in \mathbb{N}/n \geq n_0\}$.

Πράγματι, αν $S = \{m \in \mathbb{N}/m + n_0 \in S'\}$, βλέπουμε ότι $0 \in S$ και αν $m \in S$, δηλαδή $m+n_0 \in S'$, οπότε έπεται ότι $m+n_0+1 = m+1+n_0 \in S'$ και άρα $m+1 \in S$. Συνεπώς, $S = \mathbb{N}$. Άρα $S' = \{n \in \mathbb{N}/n = n_0 + m$, για κάποιο $m \in \mathbb{N}\} = \{n \in \mathbb{N}/n \geq n_0\}$.

Η ιδιότητα (1) λέγεται αρχικό βήμα και η ιδιότητα (2) λέγεται επαγωγικό βήμα.

■ **1.1.6 Εφαρμογές και Παραδείγματα. 1.** Έστω S το σύνολο όλων των

φυσικών αριθμών για τους οποίους ισχύει η σχέση

$$0+1+2+\cdots+n=\frac{1}{2}(n+1)n.$$

Να δειχθεί ότι $S=\mathbb{N}$, δηλαδή ότι η σχέση αυτή ισχύει για κάθε φυσικό αριθμό.

Σύμφωνα με την 1.1.1 αρκεί να δείξουμε ότι, το σύνολο S ικανοποιεί τις ιδιότητες (1) και (2). Πράγματι, έχουμε $0=\frac{1}{2}(0+1)\cdot 0$, δηλαδή $0\in S$. Υποθέτουμε ότι $s\in S$, δηλαδή $0+1+\cdots+s=\frac{1}{2}(s+1)s$, τότε προκύπτει ότι $s+1\in S$, αφού $0+1+\cdots+s+(s+1)=\frac{1}{2}(s+1)s+(s+1)=\frac{1}{2}((s+1)s+2(s+1))=\frac{1}{2}((s+1)+1)(s+1)$. Απ' αυτό προκύπτει ότι το άθροισμα των n πρώτων όρων μιας **αριθμητικής προόδου**

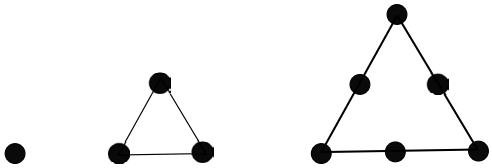
$$\alpha,\alpha+\beta,\alpha+2\beta,\ldots,\alpha+(n-1)\beta$$

ισούται με $\frac{n}{2}(2\alpha+(n-1)\beta)$.

Παρατήρηση: Λέγεται ότι ο Karl Friedrich Gauss (1777-1855) όταν ήταν μαθητής 7 ετών, ένας απ' τους καθηγητές του ζήτησε από τους μαθητές να υπολογίσουν το άθροισμα όλων των αριθμών από το 1 έως το 100. Ο Gauss αμέσως απάντησε ότι το άθροισμα είναι 5050, παρατηρώντας ότι για κάθε n ισχύει

$$\begin{aligned}2(1+2+3+\cdots+n)&=\begin{cases}1+\quad 2\quad +\quad 3\quad +\cdots+n+\\ n+n-1+n-2+\cdots+1\end{cases}\\ &=(n+1)+(n+1)+\cdots+(n+1)(n\text{ όροι }(n+1))\\ &=n(n+1).\end{aligned}$$

Η παρατήρηση αυτή του Gauss δίδει μια κομψή απόδειξη της προηγούμενης σχέσης χωρίς τη χρήση της ΑΜΕ. Σημειώνουμε ότι οι αριθμοί της μορφής $\frac{n(n+1)}{2}$ είχαν μελετηθεί από τη σχολή του Πυθαγόρα και ονομάζονται τριγωνικοί αριθμοί καθώς καθένας απ' τους αριθμούς $1=1$, $3=1+2$, $6=1+2+3,\ldots$ παριστά το πλήθος των στιγμάτων που κατανέμονται ομοιόμορφα πάνω σ' ένα ισόπλευρο τρίγωνο.



2. Έχουμε αποδεχθεί, στην αρχή του κεφαλαίου αυτού, ότι μεταξύ του 0 και 1 δεν υπάρχει άλλος φυσικός αριθμός. Μία απόδειξη αυτού μπορεί να δοθεί εφαρμόζοντας το 1.1.4 και την είς άτοπον απαγωγή. Υποθέτουμε ότι υπάρχει ένας φυσικός αριθμός α, $0 < \alpha < 1$. Πολλαπλασιάζοντας k φορές επί α, $k \in \mathbb{N}$, παίρνουμε την άπειρη γνήσια φθίνουσα ακολουθία $\alpha > \alpha > \alpha^2 > \cdots > \alpha^k > \alpha^{k+1} > \ldots$ που είναι άτοπο, σύμφωνα με την 1.1.4. Ένας άλλος τρόπος απόδειξης είναι να εφαρμόσουμε το 1.1.3 θεωρώντας το ελάχιστο στοιχείο α_0 του συνόλου όλων των φυσικών αριθμών α, $0 < \alpha < 1$. Άλλά τότε θα είχαμε $0 < \alpha_0^2 < \alpha_0 < 1$, που σημαίνει ότι το α_0 δεν είναι ελάχιστο, δηλαδή καταλήγουμε σε άτοπο.

3. ***Αρχιμήδεια Ιδιότητα.*** Αν $\alpha > 0$ και $\beta > 0$ είναι δύο ρητοί αριθμοί, τότε υπάρχει ένας φυσικός αριθμός n τέτοιος ώστε $n\alpha \geq \beta$. Εδώ μπορούμε να εφαρμόσουμε το προηγούμενο αποτέλεσμα, δηλαδή ότι ο 1 είναι το ελάχιστο στοιχείο του συνόλου των θετικών ακεραίων $\mathbb{N} - \{0\}$. Πράγματι, αν $\alpha = \dfrac{\alpha_1}{\alpha_2}$ και $\beta = \dfrac{\beta_1}{\beta_2}$ τότε, επειδή $\alpha_1\beta_2 \geq 1$, μπορούμε να πάρουμε ως n τον $\alpha_2\beta_1$ καθώς $\alpha_2\beta_1\alpha_1\beta_2 \geq \alpha_2\beta_1$ ή (διαιρώντας δια $\alpha_2\beta_2$) $\alpha_2\beta_1\dfrac{\alpha_1}{\alpha_2} \geq \dfrac{\beta_1}{\beta_2}$. Μπορούμε, επίσης, αυτό να το δείξουμε εφαρμόζοντας την Αρχή του Ελαχίστου. Έστω ότι υπάρχουν δύο θετικοί ρητοί $\alpha = \dfrac{\alpha_1}{\alpha_2}$ και $\beta = \dfrac{\beta_1}{\beta_2}$ για τους οποίους ισχύει $n\dfrac{\alpha_1}{\alpha_2} < \dfrac{\beta_1}{\beta_2}$ για κάθε $n \in \mathbb{N}$, δηλαδή $n\alpha_1\beta_2 < \alpha_2\beta_1$. Θέτουμε $r = \alpha_1\beta_2$ και $s = \alpha_2\beta_1$, και θεωρούμε το σύνολο

$$S = \{s - nr / n \in \mathbb{N}\}.$$

Το S είναι μη κενό υποσύνολο του $\mathbb{N}$ και άρα έχει ελάχιστο στοιχείο, έστω το $s - n_0 r$. Αλλά τότε και ο φυσικός αριθμός $s - (n_0 + 1)r = (s - n_0 r) - r$ είναι στοιχείο του S μικρότερος από τον $s - n_0 r$, που είναι άτοπο.

Σημειώνουμε ότι το ίδιο ισχύει αν αντί ρητών θεωρήσουμε πραγματικούς αριθμούς, αλλά για την απόδειξη χρειάζεται να χρησιμοποιήσουμε

την έννοια των "άνω φραγμάτων".

4. ***Ανάγωγα κλάσματα.*** Γνωρίζουμε οτι ένας πραγματικός αριθμός r είναι ρητός αν και μόνον αν υπάρχει ένας φυσικός αριθμός $\beta \neq 0$ τέτοιος ώστε $\beta r \in \mathbb{Z}$. Συνεπώς, αν r είναι ένας ρητός, τότε το σύνολο

$$S = \{\beta \in \mathbb{N} / \beta \neq 0, \beta r \in \mathbb{Z}\}$$

είναι μη κενό και σύμφωνα με την 1.1.3 το S έχει ένα ελάχιστο στοιχείο β_0. Αν $\beta_0 r = \alpha_0$, τότε το κλάσμα $\dfrac{\alpha_0}{\beta_0}$ είναι το ανάγωγο κλάσμα που παριστά τον ρητό αριθμό r.

5. ***Αιγυπτιακά κλάσματα.*** Πέντε χιλιάδες χρόνια πριν οι Αιγύπτιοι γνώριζαν τους αντίστροφους των φυσικών αριθμών $\dfrac{1}{n}$, $n \in \mathbb{N}$, $n \neq 0$ που ονομάζονται Αιγυπτιακά κλάσματα ή μοναδιαία κλάσματα. Οι Αιγύπτιοι δεν έγραφαν τα κλάσματα στη μορφή $\dfrac{\alpha}{\beta}$ όπως κάνουμε σήμερα, αλλά τα έγραφαν ως άθροισμα μοναδιαίων κλασμάτων. Για παράδειγμα, το κλάσμα $\dfrac{3}{4}$ το έγραφαν ως $\dfrac{1}{2} + \dfrac{1}{4}$. Ίσως αυτό το έκαναν για πρακτικούς λόγους. Μπορούσαν μ' αυτό τον τρόπο να συγκρίνουν εύκολα δύο κλάσματα, για παράδειγμα γράφοντας το $\dfrac{3}{4}$ ως $\dfrac{1}{2} + \dfrac{1}{4}$ αναγνώριζαν ότι αυτό είναι μικρότερο από το $\dfrac{4}{5}$ γράφοντάς το ως $\dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{20}$. Επίσης η γραφή αυτή των κλασμάτων τους διευκόλυνε στις εμπορικές τους συναλλαγές, για παράδειγμα, αν ήθελαν να μοιράσουν 5 σάκους σιτάρι σε 8 ανθρώπους, έγραφαν το $\dfrac{5}{8}$ ως $\dfrac{1}{2} + \dfrac{1}{8}$, οπότε ο καθένας έπαιρνε από μισό σάκο και $\dfrac{1}{8}$ του ενός σάκου.

Εδώ θα δείξουμε, ως εφαρμογή του 1.1.4, ότι

"κάθε θετικό κλάσμα $r = \dfrac{\alpha}{\beta}$, $\alpha < \beta$, γράφεται ως ένα άθροισμα διαφορετικών μοναδιαίων κλασμάτων".

Μπορούμε να υποθέσουμε ότι ο r είναι σε ανάγωγη μορφή. Θεωρούμε το μεγαλύτερο μοναδιαίο κλάσμα $\dfrac{1}{n}$ τέτοιο ώστε

$$\frac{1}{n} \leq \frac{\alpha}{\beta} < \frac{1}{n-1}.$$

Αν $\dfrac{\alpha}{\beta} = \dfrac{1}{n}$ τότε ο ισχυρισμός μας ισχύει. Αν $\alpha > 1$, τότε θεωρούμε το

κλάσμα $\frac{\alpha'}{\beta'} = \frac{\alpha}{\beta} - \frac{1}{n} = \frac{n\alpha - \beta}{n\beta}$. Επειδή $\frac{\alpha}{\beta} < \frac{1}{n-1}$ έχουμε $\alpha n - \alpha < \beta$ η $\alpha n - \beta < \alpha$. Αν το κλάσμα $\frac{n\alpha - \beta}{n\beta}$ στην ανάγωγη μορφή είναι $\frac{1}{n_1}$, τότε

$$\frac{\alpha}{\beta} = \frac{1}{n} + \frac{1}{n_1}$$

και ο ισχυρισμός μας ισχύει. Διαφορετικά θεωρούμε το μεγαλύτερο μοναδιαίο κλάσμα $\frac{1}{n_1}$, τέτοιο ώστε $\frac{1}{n_1} < \frac{\alpha n - \beta}{n\beta} < \frac{1}{n_1 - 1}$ και παίρνουμε το κλάσμα

$$\frac{\alpha''}{\beta''} = \frac{\alpha n - \beta}{n\beta} - \frac{1}{n_1} = \frac{n_1(\alpha n - \beta) - n\beta}{nn_1\beta}$$

όπου $n_1(\alpha n - \beta) - n\beta < \alpha n - \beta < \alpha$ και $\frac{\alpha}{\beta} = \frac{1}{n} + \frac{1}{n_1} + \left(\frac{\alpha n - \beta}{n\beta} - \frac{1}{n_1}\right)$. Επαναλαμβάνοντας αυτή τη διαδικασία θα παίρνουμε κλάσματα που στην ανάγωγη μορφή τους οι αριθμητές θα σχηματίζουν μια γνήσια φθίνουσα ακολουθία φυσικών αριθμών. Από το 1.1.4, αυτή η ακολουθία θα είναι πεπερασμένη και το τελευταίο κλάσμα θα έχει αριθμητή 1, δηλαδή θα είναι ένα μοναδιαίο κλάσμα. Έτσι θα έχουμε

$$\frac{\alpha}{\beta} = \frac{1}{n} + \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}, \quad n > n_1 > n_2 > \cdots > n_k$$

για κάποιο $k \in \mathbb{N}$ (το k είναι το πολύ ίσο με α, αφού στην προηγούμενη διαδικασία οι αριθμητές των ανάγωγων κλασμάτων φθίνουν). Σημειώνουμε ότι υπάρχουν πολλές παραστάσεις του $\frac{\alpha}{\beta}$ σε άθροισμα μοναδιαίων κλασμάτων, για παράδειγμα, αν στην προηγούμενη παράσταση του $\frac{\alpha}{\beta}$ θέσουμε $\frac{1}{n_i} = \frac{1}{n_i + 1} + \frac{1}{n_i(n_i + 1)}$ παίρνουμε μια διάφορη της προηγούμενης παράστασης του $\frac{\alpha}{\beta}$.

6. ***Τετραγωνικές ρίζες φυσικών αριθμών.*** Έστω $k \neq 0$ ένας φυσικός αριθμός. Θα δείξουμε ότι

"αν ο $\sqrt{k}$ δεν είναι ένας ακέραιος αριθμός, δηλαδή ο k δεν είναι το τετράγωνο ενός ακεραίου, τότε ο $\sqrt{k}$ δεν μορεί να είναι ρητός αριθμός".

Πράγματι, αν υποθέσουμε ότι ο $\sqrt{k}$ είναι ρητός, έστω $\sqrt{k} = \frac{\alpha}{\beta}$, όπου α, β είναι θετικοί ακέραιοι, τότε το σύνολο

$$S = \{n \in \mathbb{N}^* - \{0\} / n\sqrt{k} \in \mathbb{Z}\}$$

θα ήταν μη κενό, αφού $\beta\sqrt{k} = \alpha \in \mathbb{N}$. Οπότε, σύμφωνα με το 1.1.3, το S θα είχε ελάχιστο στοιχείο, έστω το m. Αλλά αν θεωρήσουμε το ακέραιο μέρος $[\sqrt{k}]$ του $\sqrt{k}$, δηλαδή το μεγαλύτερο ακέραιο που είναι μικρότερος του $\sqrt{k}$ με άλλα λόγια το μοναδικό ακέραιο $[\sqrt{k}]$ με $\sqrt{k} < [\sqrt{k}] + 1 \leq \sqrt{k} + 1$, επειδή υποθέσαμε ότι $\sqrt{k}$ δεν είναι ακέραιος, έχουμε $\sqrt{k} - [\sqrt{k}] \neq 0$, οπότε ο αριθμός $m' = m(\sqrt{k} - [\sqrt{k}])$ είναι μεγαλύτερος του μηδενός. Αλλά ο m' είναι ακέραιος, αφού ο $m\sqrt{k}$ και ο $m[\sqrt{k}]$ είναι ακέραιοι. Άρα ο m' είναι φυσικός αριθμός. Επίσης παρατηρούμε ότι, επειδή $m\sqrt{k} \in \mathbb{Z}$, ο $m'\sqrt{k} = mk - m[\sqrt{k}]\sqrt{k}$ είναι ακέραιος και άρα $m' \in S$. Αυτό είναι άτοπο καθώς $m' < m$. Άρα πρέπει το σύνολο S να είναι το κενό σύνολο.

7. ***Ρίζες πολυωνύμων με ακεραίους συντελεστές.*** Εδώ αποδεικνύουμε, εφαρμόζοντας την προηγούμενη μέθοδο ότι

"αν ένα πολυώνυμο $f(x)$ με ακεραίους συντελεστές και με το συντελεστή της μεγαλύτερης δύναμης του x ίσο με 1 έχει ρίζα έναν ρητό αριθμό r, τότε ο r πρέπει να είναι ακέραιος".

Υποθέτουμε ότι αυτό δεν ισχύει, δηλαδή ότι ο r είναι ένας μη-ακέραιος ρητός με $f(r) = r^n + \alpha_{n-1}r^{n-1} + \cdots + \alpha_0 = 0$, $\alpha_i \in \mathbb{Z}$. Τότε $r^n = -\alpha_{n-1}r^{n-1} - \cdots - \alpha_0$ και επειδή υπάρχει θετικός ακέραιος k με $kr^i \in \mathbb{Z}$, $i = 0, 1, \ldots, n-1$, το σύνολο

$$S = \{k \in \mathbb{N}^* - \{0\} / kr^s \in \mathbb{Z}, \ \ \forall\, s \in \mathbb{N}^*\}$$

είναι μη-κενό. Για κάθε $k \in S$, ισχύει (α) $k(r - [r]) \in S$ και (β) $k > k(r - [r])$. Πράγματι, επειδή $0 < r - [r] < 1$ ισχύει το (β) και $k(r - [r]) > 0$. Επίσης, επειδή $kr \in \mathbb{Z}$ θα είναι και $kr - k[r] \in \mathbb{Z}$, επιπλέον $krr - kr[r] = k(r - [r])r \in \mathbb{Z}$, αφού $kr^2 \in \mathbb{Z}$. Αυτό δίνει το (α). Μπορούμε να επαναλάβουμε την ίδια διαδικασία για το $k(r - [r])$ για να βρούμε ένα άλλο στοιχείο του S μικρότερο του $k(r - [r])$. Συνεχίζοντας με τον τρόπο αυτό θα πάρουμε μια άπειρη γνήσια φθίνουσα ακολουθία φυσικών αριθμών. Σύμφωνα με το 1.1.4, αυτό δεν μπορεί να ισχύει. Συνεπώς πρέπει $S = \emptyset$.

Σημειώνουμε ότι, μία άμεση συνέπεια του αποτελέσματος αυτού είναι ότι, η n-οστή ρίζα $\sqrt[n]{m}$ ενός φυσικού αριθμού m αν δεν είναι ακέραιος

αριθμός δεν μπορεί να είναι ρητός αριθμός.

8. Εδώ δίνουμε ένα παράδειγμα στο οποίο θα εφαρμόσουμε την πλήρη μαθηματική επαγωγή 1.1.2. Έστω $\alpha_1, \alpha_2, \dots$ μια ακολουθία πραγματικών αριθμών που ικανοποιούν τις ανισότητες $\alpha_{i+j} \leq \alpha_i + \alpha_j$, $i, j = 1, 2, \dots$. Να δειχθεί ότι ισχύει η ανισότητα

$$\alpha_1 + \frac{\alpha_2}{2} + \frac{\alpha_3}{3} + \cdots + \frac{\alpha_n}{n} \geq \alpha_n$$

για κάθε $n \in \mathbb{N}^*$.

Για $n = 1$, έχουμε την αυτοπαθή σχέση $\alpha_1 = \alpha_1$. Έστω ότι για $n = 1, 2, \dots, k$ έχουμε

$$\begin{aligned} \alpha_1 &\geq \alpha_1 \\ \alpha_1 + \frac{\alpha_2}{2} &\geq \alpha_2 \\ &\vdots \\ \alpha_1 + \frac{\alpha_2}{2} + \cdots + \frac{\alpha_k}{k} &\geq \alpha_k. \end{aligned}$$

Προσθέτοντας όλες αυτές τις ανισότητες παίρνουμε

$$k\alpha_1 + (k-1)\frac{\alpha_2}{2} + (k-2)\frac{\alpha_3}{3} + \cdots + \frac{\alpha_k}{k} \geq \alpha_1 + \alpha_2 + \cdots + \alpha_k \quad \text{ή}$$

$$k\alpha_1 + \alpha_1 + (k-1)\frac{\alpha_2}{2} + \alpha_2 + (k-2)\frac{\alpha_3}{3} + \alpha_3 + \cdots + \frac{\alpha_k}{k} + \alpha_k \geq 2(\alpha_1 + \alpha_2 + \cdots + \alpha_k)$$

ή

$$\begin{aligned} (k+1)\left(\alpha_1 + \frac{\alpha_2}{2} + \cdots + \frac{\alpha_k}{k}\right) &\geq (\alpha_1 + \alpha_k) + (\alpha_2 + \alpha_{k-1}) + \cdots + (\alpha_k + \alpha_1) \\ &\geq \alpha_{k+1} + \alpha_{k+1} + \cdots + \alpha_{k+1} = k\alpha_{k+1} \quad \text{ή} \end{aligned}$$

$$(k+1)\left(\alpha_1 + \frac{\alpha_2}{2} + \cdots + \frac{\alpha_k}{k} + \frac{\alpha_{k+1}}{k+1}\right) \geq (k+1)\alpha_{k+1}$$

οπότε

$$\alpha_1 + \frac{\alpha_2}{2} + \cdots + \frac{\alpha_{k+1}}{k+1} \geq \alpha_{k+1}.$$

Δηλαδή η ανισότητα ισχύει και για $n = k+1$. Άρα ισχύει για κάθε $n \in \mathbb{N}^*$.

9. Να δειχθεί ότι για κάθε $m \in \mathbb{N}^*$ ισχύει

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

Απόδειξη. Για $m = 1$ προφανώς ισχύει. Υποθέτουμε ότι ισχύει για $m = k$, τότε έχουμε

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

Άρα ισχύει για κάθε $m \in \mathbb{N}^*$.

- *Εφαρμογή*: Έστω $m, n \in \mathbb{N}^*$, τότε ο m^n είναι το άθροισμα m περιττών διαδοχικών αριθμών. Πράγματι, έστω

$$\begin{aligned} m^n &= (2k+1) + (2k+3) + \cdots + (2k+2m-1) \\ &= 2km + (1 + 3 + \cdots + 2m - 1) \\ &= 2km + m^2, \quad \text{οπότε} \end{aligned}$$

$$k = \frac{m(m^{n-2} - 1)}{2}.$$

Επειδή αν ένας απ' τους m και $m^{n-2} - 1$ είναι περιττός ο άλλος είναι άρτιος, ο αριθμός k είναι φυσικός και δίνει την παράσταση του m^n ως άθροισμα m περιττών διαδοχικών αριθμών.

10. ***Ταυτότητες.*** Για κάθε $x, y \in \mathbb{C}$ και $n \in \mathbb{N}$ ισχύει

(α) $$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$$

και για n περιττό ισχύει

(β) $$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$$

Απόδειξη. (α) Για $n = 1$ προφανώς ισχύει. Απ' το επαγωγικό βήμα έχουμε

$$\begin{aligned} x^{n+1} - y^{n+1} &= x^n x - y^n y + x^n y - x^n y \\ &= x^n(x-y) + y(x^n - y^n) \\ &= x^n(x-y) + y(x-y)(x^{n-1} + \cdots + y^{n-1}) \\ &= (x-y)(x^n + x^{n-1}y + \cdots + y^n). \end{aligned}$$

(β) Αν ο n είναι περιττός, τότε θέτοντας στην προηγούμενη σχέση αντί y το $-y$ παίρνουμε το ζητούμενο.

- *Εφαρμογή*: Δείξτε ότι $(\alpha + \beta\sqrt{r})^n + (\alpha - \beta\sqrt{r})^n \in \mathbb{Z}$.
- *Εφαρμογή*: Στα επόμενα θα χρειαστούμε το άθροισμα μιας ακολουθίας

αριθμών $\alpha, \alpha r, \alpha r^2, \ldots, \alpha r^n \ldots \alpha, r \in \mathbb{R}$. Η ακολουθία αριθμών $\alpha, \alpha r, \alpha r^2, \ldots, \alpha r^n, \ldots$ λέγεται **γεωμετρική πρόοδος**. Το άθροισμα των $n+1$ πρώτων όρων

$$\sum_{i=0}^{n} \alpha r^i = \alpha \sum_{i=0}^{n} r^i,$$

σύμφωνα με την ταυτότητα (α), ισούται με

$$\alpha \sum_{0}^{n} r^i = \alpha(1 + r + \cdots + r^n) = \alpha \frac{r^{n+1} - 1}{r - 1} = \alpha \frac{1}{1 - r} + \alpha \frac{r^{n+1}}{1 - r}.$$

Αν $|r| < 1$, τότε $\lim\limits_{n \to \infty} r^{n+1} = 0$, οπότε

$$\lim_{n \to \infty} \alpha \sum_{0}^{n} r^i = \alpha \sum_{0}^{\infty} r^i = \frac{\alpha}{1 - r}.$$

Δηλαδή η σειρά $\alpha \sum\limits_{0}^{\infty} r^i$ συγκλίνει στο $\dfrac{\alpha}{1 - r}$.

11. ***Παράδοξα.*** Κατά την εφαρμογή της ΑΜΕ πρέπει να είμαστε προσεκτικοί ούτως ώστε οι ισχυρισμοί μας να είναι απολύτως σωστοί, διαφορετικά προκύπτουν λογικά παράδοξα.

Για παράδειγμα, ας υποθέσουμε ότι θέλουμε να δείξουμε ότι $2 \cdot n = 0$, για κάθε $n \in \mathbb{N}$. Για $n = 0$ αυτό ισχύει. Έστω ότι ισχύει για k, $0 \leq k \leq n$. Γράφουμε $n + 1 = \alpha + \beta$, $\alpha < n + 1$, $\beta < n + 1$ $\alpha, \beta \in \mathbb{N}$. Οπότε $6(n+1) = 6(\alpha + \beta) = 6\alpha + 6\beta = 0$, αφού $6\alpha = 6\beta = 0$, από την υπόθεση. Αυτό το παράδοξο αποτέλεσμα προέκυψε επειδή δεν λάβαμε υπόψιν μας ότι ο αριθμός 1 δεν μπορεί να γραφεί ως άθροισμα δύο φυσικών αριθμών $\neq 0$.

Ένα άλλο παράδειγμα είναι το γνωστό παράδοξο "τα άλογα του Polya". Ο γνωστός Ούγγρος μαθηματικός G. Polya έθεσε την εξής άσκηση. Να βρεθεί το λάθος στον ισχυρισμό μέσω του οποίου αποδεικνύουμε με την ΑΜΕ ότι όλα τα άλογα έχουν το ίδιο χρώμα. Το αρχικό βήμα ισχύει, αφού έχουμε ένα άλογο. Υποθέτουμε ότι σε κάθε αγέλη n αλόγων όλα τα άλογα έχουν το ίδιο χρώμα. Έστω μια αγέλη αλόγων με $n + 1$ άλογα. Αν αριθμήσουμε τα άλογα και θεωρήσουμε τα πρώτα n απ' αυτά, τότε επαγωγικά αυτά έχουν το ίδιο χρώμα. Επίσης τα n τελευταία άλογα απ'

αυτά έχουν το ίδιο χρώμα. Επειδή αυτές οι δύο αγέλες αλόγων έχουν κοινά άλογα, όλα και τα $n+1$ άλογα έχουν το ίδιο χρώμα. Άρα όλα τα άλογα, όπου υπάρχουν, έχουν το ίδιο χρώμα. Το λάθος στον ισχυρισμό μας είναι ότι σιωπηρά θεωρήσαμε τις δύο αγέλες να έχουν κοινά άλογα. Αυτό ισχύει όταν το n είναι ≥ 3. Αν $n = 2$ ο ισχυρισμός δεν ισχύει και συνεπώς η εφαρμογή της ΑΜΕ ήταν ελλειπής και άρα εσφαλμένη.

1.2 Διαιρετότητα

Η βασικότερη έννοια στην οποία βασίζονται όλα όσα ακολουθούν είναι η εξής:

1.2.1 Ορισμός. *Έστω $\alpha, \beta \in \mathbb{Z}$. Θα λέμε ότι ο ακέραιος β διαιρεί τον ακέραιο α (ή ότι ο α διαιρείται δια του β) αν υπάρχει ένας ακέραιος γ τέτοιος ώστε*

$$\alpha = \beta\gamma$$

Σ' αυτή την περίπτωση επίσης λέμε ότι ο α είναι ένα πολλαπλάσιο του β ή ότι ο β είναι ένας διαιρέτης του α ή ότι ο β είναι ένας (πολλαπλασιαστικός) παράγοντας του α και θα γράφουμε "$\beta \mid \alpha$". Διαφορετικά, δηλαδή αν ο β δεν διαιρεί τον α, θα γράφουμε $\beta \nmid \alpha$.

Παραδείγματος χάριν, το 3 διαιρεί το -18 καθώς $-18 = 3(-6)$ και το 3 διαιρεί το 333333 αφού $33333 = 3(11111)$. Επίσης το 6 διαιρεί το 0, αφού $0 = 6 \cdot 0$ ενώ το $3 \nmid 5$.

1.2.2 Παρατήρηση. **1.** Στο προηγούμενο ορισμό, αν ο $\beta \neq 0$, τότε ο γ ορίζεται μοναδικά (λόγω της ισχύος του νόμου απαλειφής στους ακέραιους, αλλά και λόγω της "διαίρεσης με υπόλοιπο" του Ευκλείδη του 1.2.7 πιο κάτω).

2. Αν $\beta = 0$ τότε απ' την ισότητα $\alpha = 0 \cdot \gamma$ συνεπάγεται ότι $\alpha = 0$, άρα ο μόνος ακέραιος α ο οποίος είναι πολλαπλάσιο του 0 είναι το 0 και η ισότητα $0 = 0 \cdot \gamma$ ισχύει για κάθε γ. Προσοχή όμως, η έκφραση $0 \mid 0$ (αυτή που μόλις ορίσθηκε) έχει διαφορετική έννοια απ' την έκφραση $\frac{0}{0}$, καθώς το $\frac{0}{0}$ παριστά υποτίθεται ένα κλάσμα που δεν ορίζεται.

Διατυπώνουμε τώρα τις βασικές ιδιότητες της διαιρετότητας. Παρότι αυτές μπορεί να είναι γνωστές ή προφανείς, δίνουμε τις αποδείξεις τους θεωρώντας ότι είναι διδακτικές όσον αφορά τον τρόπο με τον οποίο επιχειρηματολογούμε για να λύνουμε προβλήματα.

1.2.3 Πρόταση. (Βασικές ιδιότητες)

i) *Έστω* $\alpha \in \mathbb{Z}$, *με* $\alpha \neq 0$. *Τότε* $\alpha \mid \pm\alpha$.

ii) *Οι ακέραιοι* 1 *και* -1 *είναι διαιρέτες κάθε ακεραίου.*

iii) *Αν* $\alpha, \beta \in \mathbb{Z}$ *και* $\beta \mid \alpha$, *τότε* $\beta \mid -\alpha$, $-\beta \mid \alpha$, $-\beta \mid \alpha$ *και* $|\beta| \Big| |\alpha|$, *(όπου* $|x|$ *συμβολίζει την απόλυτη τιμή του ακέραιου* x*).*

iv) *Αν* $\alpha, \beta, \gamma \in \mathbb{Z}$ *και* $\beta \mid \alpha$, $\alpha \mid \gamma$, *τότε* $\beta \mid \gamma$ *(μεταβατική ιδιότητα).*

v) *Αν* $\alpha, \beta, \gamma \in \mathbb{Z}$ *με* $\gamma \neq 0$ *και* $\beta\gamma \mid \alpha\gamma$, *τότε* $\beta \mid \alpha$.

vi) *Αν* $\alpha, \beta \in \mathbb{Z}$ *και* $\beta \mid \alpha$, *τότε* $\beta \mid \alpha\gamma$ *και* $\beta\gamma \mid \alpha\gamma$, $\forall\, \gamma \in \mathbb{Z}$.

vii) *Αν* $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ *και* $\beta \mid \alpha$, $\delta \mid \gamma$, *τότε* $\beta\delta \mid \alpha\gamma$.

viii) *Αν* $\alpha, \beta, \gamma \in \mathbb{Z}$ *και* $\beta \mid \alpha$, $\beta \mid \gamma$, *τότε* $\beta \mid \alpha k + \gamma\lambda$, *για κάθε* $k, \lambda \in \mathbb{Z}$.

ix) *Αν* $\alpha, \beta \in \mathbb{Z}$ *με* $\alpha \neq 0$ *και* $\beta \mid \alpha$ *τότε* $|\beta| \leq |\alpha|$. *Συνεπώς αν* $\beta \mid \alpha$ *και* $\alpha \mid \beta$, *τότε* $|\alpha| = |\beta|$.

x) *Αν* $\alpha, \beta \in \mathbb{Z}$, *με* $\alpha \neq 0$ *και* $\beta \mid \alpha$, *τότε* $\dfrac{\alpha}{\beta} \mid \alpha$.

Απόδειξη. Οι i) και ii) προκύπτουν απ' τις ισότητες $\alpha = \alpha \cdot 1$, $-\alpha = \alpha \cdot (-1)$ και $\alpha = -\alpha(-1)$.

iii) Καθώς $\beta \mid \alpha$, υπάρχει $\gamma \in \mathbb{Z}$ με $\alpha = \beta\gamma$. Οπότε ισχύει $-\alpha = \beta(-\gamma)$, $\alpha = (-\beta)(-\gamma)$, $-\alpha = (-\beta) \cdot \gamma$ και $|\alpha| = |\beta\gamma| = |\beta|\,|\gamma|$.

iv) Αν $\alpha = \beta\gamma'$ και $\gamma = \alpha\gamma''$, $\gamma', \gamma'' \in \mathbb{Z}$, τότε $\gamma = \beta\gamma'\gamma''$.

v) Αν $\alpha\gamma = \beta\gamma\gamma'$, $\gamma' \in \mathbb{Z}$, τότε $\gamma(\alpha - \beta\gamma') = 0$. Καθώς $\gamma \neq 0$, απ' τον νόμο απαλειφής προκύπτει $\alpha = \beta\gamma'$.

vi) Αν $\alpha = \beta\gamma'$, $\gamma' \in \mathbb{Z}$, τότε $\alpha\gamma = \beta\gamma\gamma'$, οπότε $\beta \mid \alpha\gamma$ και $\beta\gamma \mid \alpha\gamma$.

vii) Αν $\alpha = \beta\gamma'$ και $\gamma = \delta\gamma''$, τότε $\alpha\gamma = \beta\delta\gamma'\gamma''$.

viii) Πρέπει να δείξουμε ότι υπάρχει ένας ακέραιος λ' τέτοιος ώστε $\alpha k + \gamma\lambda = \beta\lambda'$. Αλλά $\alpha = \beta\lambda_1$ και $\gamma = \beta\lambda_2$ για κάποια $\lambda_1, \lambda_2 \in \mathbb{Z}$. Οπότε $\alpha k + \gamma\lambda = \beta\lambda_1 k + \beta\lambda_2\lambda = \beta(\lambda_1 k + \lambda_2\lambda)$, όπου $\lambda_1 k + \lambda_2\lambda \in \mathbb{Z}$.

ix) Ισχύει $\alpha = \beta\gamma$, για κάποιο $\gamma \in \mathbb{Z}$ και άρα $|\alpha| = |\beta|\,|\gamma|$. Καθώς $\alpha \neq 0$ προκύπτει ότι $\gamma \neq 0$. Άρα $|\gamma| \geq 1$ και συνεπώς $|\alpha| \geq |\beta|$.

x) Καθώς $\alpha \neq 0$, πρέπει $\beta \neq 0$. Έχουμε $\alpha = \beta\gamma$, για κάποιο $\gamma \in \mathbb{Z}$. Τότε $\gamma = \dfrac{\alpha}{\beta} | \alpha$. □

1.2.4 Πόρισμα. *Το πλήθος των διαιρετών ενός μη μηδενικού ακεραίου α είναι πεπερασμένο. Αν ο α δεν είναι ένα τέλειο τετράγωνο, τότε το πλήθος αυτό είναι άρτιο.*

Απόδειξη. Απ' την ιδιότητα ix), αν β είναι ένας διαιρέτης του α, τότε $|\beta| \leq |\alpha|$, οπότε $\beta \in \{-\alpha, -\alpha+1, \ldots, -1, 1, \ldots, \alpha-1, \alpha\}$. Δηλαδή ο α έχει το πολύ $2|\alpha|$ διαιρέτες, (οπότε ο μόνος ακέραιος ο οποίος έχει άπειρους διαιρέτες είναι το 0), αφού $0 = 0\gamma$, $\forall\, \gamma \in \mathbb{Z}$).

Απ' την ιδιότητα x) προκύπτει ότι, αν β είναι ένας διαιρέτης του α τότε και ο $\dfrac{\alpha}{\beta}$ είναι διαιρέτης του α. Αν ο α δεν είναι το τετράγωνο ενός ακέραιου και $\beta \mid \alpha$, τότε $\beta \neq \dfrac{\alpha}{\beta}$. Συνεπώς, οι διαιρέτες του α απαριθμούνται σε ζεύγη $\left(\beta, \dfrac{\alpha}{\beta}\right)$ με $\beta \neq \dfrac{\alpha}{\beta}$, $\beta \mid \alpha$ και άρα το πλήθος των διαιρετών του είναι άρτιο. □

1.2.5 Παρατήρηση. Η ιδιότητα iii) αναφέρει ότι "$\beta \mid \alpha$ αν και μόνο αν $|\beta| \mid |\alpha|$". Συνεπώς, η διαιρετότητα στους ακέραιους ανάγεται στη διαιρετότητα στους μη αρνητικούς ακέραιους. Γι αυτό το λόγο συχνά, όταν μελετάμε προβλήματα διαιρετότητας μπορούμε να περιοριζόμεθα στους μη αρνητικούς αριθμούς.

☞ **1.2.6 Παραδείγματα. 1.** Να βρεθούν όλοι οι θετικοί ακέραιοι n για τους οποίους ισχύει

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

Έστω ότι υπάρχει $\alpha \in \mathbb{Z}$ τέτοιος ώστε $n^2+1 = \alpha(n+1)$. Επειδή $n^2+1 = (n+1)(n-1)+2$, προκύπτει ότι $(\alpha-(n-1))(n+1) = 2$. Άρα $(n+1) \mid 2$. Συνεπώς πρέπει $n+1 = 1$ ή $n+1 = 2$ και επειδή $n \geq 1$, η λύση είναι $n = 1$.

2. Αν ο n είναι άρτιος φυσικός αριθμός, τότε ο 4 διαιρεί τον n^2+2n+4. Πράγματι, απ' την ιδιότητα vii) επειδή το $2 \mid n$ έχουμε ότι το $4 \mid n^2$ και επειδή το $2 \mid 2$ και το $2 \mid n$, έχουμε ότι $4 \mid 2n$ (ιδιότητα vi)). Συνεπώς $4 \mid n^2+2n$ (ιδιότητα viii)) και $4 \mid n^2+2n+4$.

Μία άλλη απόδειξη είναι η εξής: Επειδή $2 \mid (n+2)$ έχουμε ότι $4 \mid (n+2)^2$. Αλλά $4 \mid 2n$ και άρα $4 \mid (n+2)^2 - 2n = n^2+2n+4$.

3. Δείχνουμε, εφαρμόζοντας επαγωγή στο n, ότι, $5 \mid (2^{4n+2}+1)$. Προφανώς για $n = 0$ ισχύει. Υποθέτουμε ότι ισχύει για n και δείχνουμε ότι ισχύει και για $n+1$. Πράγματι, επειδή $5 \mid -15 = 1-2^4$ και $5 \mid (2^{4n+2}+1)$ θα πρέπει

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

4. Το γινόμενο n διαδοχικών ακέραιων διαιρείται δια του $n!$. Υποθέτουμε ότι όλοι οι διαδοχικοί ακέραιοι $m+1, m+2, \ldots, m+n$ είναι θετικοί. Οπότε έχουμε

$$\binom{m+n}{n} = \frac{(m+1)(m+2)\cdots(m+n)}{n!} \in \mathbb{Z}.$$

Αν οι k απ' αυτούς δεν είναι θετικοί, τότε το προηγούμενο γινόμενο $(m+1)\cdots(m+n)$ πολλαπλασιασμένο με $(-1)^k$ διαιρείται δια $n!$, οπότε και το αρχικό διαιρείται δια $n!$. Για παράδειγμα το $3! = 6$ διαιρεί κάθε αριθμό της μορφής $n(n-1)(n+1) = n^3-n$, ενώ το $120 = 5!$ διαιρεί κάθε αριθμό της μορφής $n^5-5n^3+4n = (n-2)(n-1)n(n+1)(n+2)$.

5. Το άθροισμα n διαδοχικών ακεραίων διαιρείται δια n αν και μόνον αν ο n είναι περιττός.

Πράγματι, γνωρίζουμε ότι το άθροισμα μιας αριθμητικής προόδου α, $\alpha+d$, $\alpha+2d, \ldots, \alpha+(n-1)d$ είναι ίσο με

$$\frac{n(\text{αρχικός όρος} + \text{τελευταίος όρος})}{2} = \frac{n(\alpha+\alpha+(n-1)d)}{2}.$$

Έστω $\alpha, \alpha+1, \ldots, \alpha+(n-1)$ n διαδοχικοί ακέραιοι, τότε

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

Αν $n = 2m+1$ τότε το άθροισμα είναι

$$\frac{(2m+1)(2\alpha+2m+1-1)}{2} = \frac{(2m+1)(2\alpha+2m)}{2} = (2m+1)(\alpha+m)$$

Αν $n = 2m$ το άθροισμα γίνεται

$$\frac{2m(2\alpha+2m-1}{2} = 2m\alpha + 2m^2 - m.$$

Καθώς $2m \mid 2m\alpha$, $2m \mid 2m^2$ και $2m \nmid m \Rightarrow 2m \nmid 2m\alpha + 2m^2 - m$.

Το επόμενο θεώρημα, που μας είναι γνωστό από τα μαθητικά μας χρόνια, αποτελεί τη θεμελιώδη ιδιότητα της διαιρετότητας πάνω στην οποία στηρίζεται όλη η ανάπτυξη της στοιχειώδους θεωρίας αριθμών.

1.2.7 Θεώρημα. (Ευκλείδεια διαίρεση με υπόλοιπο). *Έστω $\alpha, \beta \in \mathbb{Z}$ με $\beta \neq 0$. Τότε υπάρχουν μοναδικοί ακέραιοι π και υ τέτοιοι ώστε*

$$\alpha = \beta\pi + \upsilon \quad \textit{και} \quad 0 \leq \upsilon < |\beta|.$$

Το π ονομάζεται **πηλίκο** και το υ **υπόλοιπο**. Λόγω της μοναδικότητας, όταν αναφερόμαστε στο π και το υ, μπορούμε να λέμε **το** πηλίκο και **το** υπόλοιπο της Ευκλείδειας διαίρεσης του α δια του β.

Απόδειξη. Πρώτα δείχνουμε την ύπαρξη του π και του υ. Θεωρούμε το σύνολο Σ όλων των ακέραιων της μορφής $\alpha + k\beta$, $k \in \mathbb{Z}$, δηλαδή

$$\Sigma = \{\ldots, \alpha-2\beta, \alpha-\beta, \alpha, \alpha+\beta, \alpha+2\beta, \ldots\} = \{\alpha + k\beta / k \in \mathbb{Z}\}.$$

Το υποσύνολο $S = \Sigma \cap \mathbb{N}$ του $\mathbb{N}$ των μη αρνητικών ακέραιων του Σ είναι μη-κενό, αφού για παράδειγμα $\alpha + (|\alpha|+1)|\beta| \in S$, ή εναλλακτικά αν $\alpha \geq 0$, τότε επιλέγουμε $k = 0$ και αν $\alpha < 0$, τότε επιλέγουμε $k = -\alpha\beta$. Συνεπώς, σύμφωνα με την αρχή του ελαχίστου, το S περιέχει ένα ελάχιστο στοιχείο υ. Έστω $\upsilon = \alpha + k\beta$, οπότε $\alpha = \beta\pi + \upsilon$, όπου $\pi = -k \in \mathbb{Z}$.

Τότε πρέπει να ισχύει $0 \leq \upsilon < |\beta|$. Διότι διαφορετικά θα είχαμε $\upsilon \geq |\beta|$. Οπότε ο ακέραιος

$$0 \leq \upsilon - |\beta| = \begin{cases} \alpha + \beta(-(\pi+1)) & \text{αν} \quad \beta > 0 \\ \alpha + \beta(1-\pi) & \text{αν} \quad \beta < 0 \end{cases}$$

θα ήταν ένα στοιχείο του S. Αυτό δεν μπορεί να ισχύει διότι $\upsilon - |\beta| < \upsilon$ και το υ είναι ο ελάχιστος ακέραιος του S.

Για τη μοναδικότητα των π και υ, υποθέτουμε ότι έχουμε τις ισότητες

$$\alpha = \beta\pi_1 + \upsilon_1, \quad 0 \leq \upsilon_1 < |\beta|$$
$$\alpha = \beta\pi_2 + \upsilon_2, \quad 0 \leq \upsilon_2 < |\beta|.$$

Αφαιρώντας αυτές τις ισότητες παίρνουμε

$$\beta(\pi_1 - \pi_2) = \upsilon_2 - \upsilon_1.$$

Αλλά προσθέτοντας τις ανισότητες $0 \leq \upsilon_1 < |\beta|$ και $-|\beta| < -\upsilon_2 \leq 0$ παίρνουμε $|\upsilon_2 - \upsilon_1| < |\beta|$. Οπότε έχουμε $|\beta|\,|\pi_1 - \pi_2| = |\upsilon_2 - \upsilon_1| < |\beta|$. Αλλά το μόνο ακέραιο πολλαπλάσιο του $|\beta|$ που είναι μικρότερο απ' το $|\beta|$ είναι το μηδέν, δηλαδή πρέπει $|\beta|\,|\pi_1 - \pi_2| = 0$ ή $\pi_1 = \pi_2$ και άρα $\upsilon_1 = \upsilon_2$. □

1.2.8 Παρατηρήσεις. **1.** Ένα κύριο συμπέρασμα στο θεώρημα είναι οι ανισότητες που αναφέρονται για το υ. Δηλαδή ότι το υπόλοιπο της διαίρεσης είναι ο μικρότερος μη-αρνητικός ακέραιος της μορφής $\alpha - \beta\pi$.

2. Αν το υπόλοιπο $\upsilon = 0$, τότε $\alpha = \beta\pi$, δηλαδή $\beta \mid \alpha$, όπου το π είναι μοναδικό (σύμφωνα με το θεώρημα). Αυτό μας δίνει μια διαφορετική απόδειξη της μοναδικότητας που αναφέρεται στην Παρατήρηση του 1.2.2.

3. Στη διατύπωση του θεωρήματος απαιτούμε να είναι $\beta \neq 0$, διότι διαφορετικά αν $\alpha > 0$ θα είχαμε $\alpha = 0 \cdot \pi + \alpha$, δηλαδή δεν θα ικανοποιείτο η ανισότητα για το υπόλοιπο. Επίσης αν $\alpha = 0$ και $\beta = 0$ τότε πάλι θα είχαμε $0 = 0 \cdot \pi$, όπου το π δεν είναι μοναδικό.

4. Αν και το Θεώρημα 1.2.7 είναι ένα θεώρημα "ύπαρξης και μο-

ναδικότητας" πολλές φορές αναφέρεται ως ο "Αλγόριθμος Διαίρεσης"[1]. Εδώ αυτή η ονομασία δικαιολογείται απ' την απόδειξη του 1.2.7, καθώς μπορούμε να καθορίσουμε το υπόλοιπο ξεκινώντας από μια μη αρνητική διαφορά $\alpha - k\beta \geq 0$ και διαδοχικά να αφαιρούμε πολλαπλάσια του β τόσες φορές όσες απαιτούνται για να φθάσουμε σε μια τέτοια διαφορά που να είναι μικρότερη του $|\beta|$, δηλαδή στο υπόλοιπο $\upsilon = \alpha - \beta\pi$.

5. Υπενθυμίζουμε ότι ως μαθητές στο σχολείο μαθαίνουμε να διαιρούμε έναν ακέραιο α δια ενός θετικού ακεραίου β εφαρμόζοντας την εξής αλγοριθμική μέθοδο: Έστω ότι ο α έχει $n+1$ ψηφία $\alpha_n, \alpha_{n-1}, \ldots, \alpha_0$, δηλαδή $\alpha = \alpha_n\alpha_{n-1}\ldots\alpha_0$ είναι η δεκαδική παράσταση του α (βλέπε αμέσως πιο κάτω). Στη διαίρεση του σχολείου εκτελούμε $n+1$ βήματα καθώς κάθε ψηφίο του α απαιτεί ακριβώς ένα βήμα που δίνει ένα ψηφίο του πηλίκου. Συγκεκριμένα, το βήμα i εκτελείται ως εξής: Βρίσκουμε το μεγαλύτερο ακέραιο π_i τέτοιον ώστε ο $\beta\pi_i$ να μην είναι μεγαλύτερος του A_i, όπου ο A_i ορίζεται ως εξής:

$$A_n = \alpha_n, \quad A_i = 10(A_{i+1} - \beta\pi_{i+1}) + \alpha_i, \quad 0 \leq i < n.$$

Γράφουμε π_i στα δεξιά του π_{i+1}. Μετά το βήμα $i = 0$, αυτό που μένει είναι το υπόλοιπο υ. Στη διαδικασία αυτή ο διαιρεθέντας αριθμός α πρέπει να ισούται με το άθροισμα του υπολοίπου και όλων των αριθμών που έχουν αφαιρεθεί. Αλλά οι αριθμοί που αφαιρούνται είναι οι $\beta\pi_i$ επί 10^i. Συνεπώς,

$$\begin{aligned}\alpha &= \beta\pi_n 10^n + \beta\pi_{n-1}10^{n-1} + \cdots + \beta\pi_1 10 + \beta\pi_0 + \upsilon \\ &= \beta(\pi_n\pi_{n-1}\cdots\pi_0) + \upsilon, \quad \text{όπου} \quad 0 \leq \upsilon < \beta.\end{aligned}$$

Έτσι βλέπουμε ότι η διαίρεση του σχολείου μας δίνει το σωστό πηλίκο και υπόλοιπο της Ευκλείδειας διαίρεσης. Για παράδειγμα, έστω $\alpha = 4785$ και $\beta = 16$. Έχουμε $A_4 = 4$ και $\pi_4 = 0$. $A_3 = 10(4 - 16\cdot 0) + 7 = 47$, $\pi_3 = 2$, $A_2 = 10(47 - 16\cdot 2) + 8 = 158$, $\pi_2 = 9$, $A_1 = 10(158 - 16\cdot 9) + 5 = 145$, $\pi_1 = 9$, $A_0 = 10(145 - 16\cdot 9) = 1$. Συνεπώς $\alpha = 16\cdot 199 + 1$, όπου $\pi = 199$, $\upsilon = 1$.

[1] Αλγόριθμος είναι μια διαδικασία που λύνει ένα πρόβλημα μέσω μιας πεπερασμένης ακολουθίας καθορισμένων βημάτων.

Πρέπει εδώ να τονίσουμε ότι στο σχολείο δεν γράφουμε τη διαίρεση του α δια του β ως $\alpha = \beta\pi + \upsilon$, αλλά συνήθως ως $\frac{a}{\beta} = \pi + \frac{\upsilon}{\beta}$ εννοώντας τη διαίρεση ως "πράξη" λαμβάνοντας ως αποτέλεσμα έναν ρητό αριθμό. Εδώ όμως όταν διαιρούμε τον α δια του β δεν εννοούμε την πράξη της διαίρεσης αλλά θεωρούμε ακριβώς αυτό που αναφέρεται στο Θεώρημα 1.2.7, καθώς στους ακέραιους αριθμούς δεν ορίζεται η πράξη της διαίρεσης.

6. Υποθέτουμε ότι $\alpha > 0$ και $\beta > 0$ και έστω $\alpha = \beta\pi + \upsilon$, $0 \leq \upsilon < \beta$. Τότε το πλήθος των θετικών πολλαπλασίων του β που είναι μικρότερα ή ίσα του α είναι ακριβώς π.

Πράγματι, ένα θετικό πολλαπλάσιο $\lambda\beta$ του β είναι μικρότερο ή ίσο του α αν και μόνον αν $0 < \lambda \leq \frac{\alpha}{\beta}$. Αλλά $\frac{\alpha}{\beta} = \pi + \frac{\upsilon}{\beta}$. Άρα το πλήθος των φυσικών αριθμών που είναι μικρότεροι ή ίσοι του $\frac{\alpha}{\beta}$ είναι π αφού $0 \leq \upsilon < \beta$, δηλαδή $0 \leq \frac{\upsilon}{\beta} < 1$. Η ισότητα $\frac{\alpha}{\beta} = \pi + \frac{\upsilon}{\beta}$ επίσης δείχνει ότι ο π είναι ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος του $\frac{\alpha}{\beta}$.

Αν x είναι ένας πραγματικός αριθμός, **το ακέραιο μέρος** του x, που συμβολίζεται[2] με $[x]$, ορίζεται ως ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος του x, π.χ. $[2] = 2$, $[0,2] = 0$, $[-5,2] = -6$. Συνεπώς, στη συγκεκριμένη περίπτωση έχουμε "$\left[\frac{\alpha}{\beta}\right] = \pi =$ πλήθος θετικών πολλαπλασίων του β που είναι μικρότερα ή ίσα του α".

☞ **1.2.9 Παραδείγματα. 1.** Αν διαιρέσουμε το 59 δια του 7 έχουμε $59 = 7 \cdot 8 + 3$, $\pi = 8$, $\upsilon = 3$. Επίσης έχουμε

$$\begin{aligned} -59 &= 7 \cdot (-9) + 4, && \pi = -9, && \upsilon = 4 < 7 \\ 59 &= (-7)(-8) + 3, && \pi = -8. && \upsilon = 3 < |-7| = 7 \\ -59 &= (-7)(9) + 4, && \pi = 9, && \upsilon = 4 < |-7| = 7. \end{aligned}$$

2. Σύμφωνα με τη διαίρεση του Ευκλείδη 1.2.7, αν διαιρέσουμε έναν ακέραιο α δια του 4, παίρνουμε τέσσερα δυνατά υπόλοιπα: το 0, το 1, το 2 και το 3. Αυτό σημαίνει ότι ο α μπορεί να γραφεί σε μια από τις εξής

[2] Ο συμβολισμός αυτός υιοθετήθηκε απ' τον Gauss το 1808 στην τρίτη απόδειξη που έδωσε για το νόμο αντιστροφής που θα μελετήσουμε στο Κεφάλαιο 4.

μορφές:

$$\alpha = 4\pi + 0, \quad \alpha = 4\pi + 1, \quad \alpha = 4\pi + 2, \quad \alpha = 4\pi + 3.$$

Γενικά, αν διαιρέσουμε τον α δια ενός ακεραίου n τότε το υπόλοιπο της διαίρεσης θα είναι ένας από τους n αριθμούς $0, 1, 2, \ldots, n-1$. Αυτό σημαίνει ότι η διαίρεση του Ευκλείδη ταξινομεί όλους τους ακέραιους σ' αυτούς που αφήνουν υπόλοιπο 0, σ' αυτούς που αφήνουν υπόλοιπο $1, \ldots$, και σ' αυτούς που αφήνουν υπόλοιπο $n-1$. Για παράδειγμα, αν $n = 2$, τότε οι ακέραιοι ταξινομούνται στους άρτιους, δηλαδή σ' αυτούς που αφήνουν υπόλοιπο 0 και στους περιττούς, δηλαδή σ' αυτούς που αφήνουν υπόλοιπο 1. Άρα ένας ακέραιος είναι ή άρτιος ή περιττός. Σ' αυτή την ιδέα της ταξινόμησης των ακεραίων βασίζεται η αριθμητική των ισοτιμιών (ή υπολοίπων) που αναπτύχθηκε από τον Gauss και θα μελετήσουμε στο επόμενο κεφάλαιο.

3. Υπενθυμίζουμε ότι ένας πραγματικός αριθμός r είναι ρητός αν και μόνον αν $r = \dfrac{\alpha}{\beta}, \alpha, \beta \in \mathbb{Z}$, $\beta \neq 0$. Ένας πραγματικός αριθμός που δεν είναι ρητός λέγεται άρρητος. Είναι γνωστό ότι ο πρώτος που απέδειξε την ύπαρξη των άρρητων αριθμών ήταν ο Πυθαγόρας[3] (ή η Σχολή του) ο οποίος μέσω του Πυθαγόριου Θεωρήματος απέδειξε ότι ο $\sqrt{2}$ δεν είναι ρητός. Ιστορικά αυτό το αποτέλεσμα είναι ένα από τα πιο σημαντικά θεωρήματα[4] των μαθηματικών, αν και σήμερα θεωρείται φυσιολογικό αποτέλεσμα. Εδώ δίνουμε ως δεύτερη απόδειξη (άλλες δίδονται στα επόμενα) του γεγονότος αυτού, χρησιμοποιώντας το διαχωρισμό των φυσικών αριθμών σε άρτιους και περιττούς. Υποθέτουμε ότι $\sqrt{2} = \dfrac{\alpha}{\beta}$, $\alpha, \beta \in \mathbb{Z}$. Απαλείφοντας τους

[3] Ο αριθμός $\sqrt{2}$ είναι ο πρώτος άρρητος αριθμός που βρέθηκε στα χρονικά της ιστορίας. Ανακαλύφθηκε από τους Πυθαγόρειους πριν 2600 χρόνια. Μέχρι τότε οι αρχαίοι πίστευαν ότι δεν υπάρχουν άλλοι αριθμοί εκτός απ' τους ρητούς. Αποδεικνύοντας οι Πυθαγόρειοι ότι ο "άγνωστος αριθμός $\sqrt{2}$" δεν είναι ρητός δημιουργήθηκε ένα κενό στην κοσμοθεωρία τους η οποία βασιζόταν στους αριθμούς. Γι' αυτό το λόγο λέγεται ότι κρατούσαν όρκο σωπής για την ύπαρξη του $\sqrt{2}$. Αλλά ένας απ' αυτούς ο Ίππασος ο Μεταπόντιος αποκάλυψε δημόσια το μυστικό τους, αλλά όπως λέει ο μύθος ο ίδιος ο Πυθαγόρας τον καταδίωξε και τον έπνιξε στη θάλασσα.

[4] Αυτό είναι ένα απ' τα δύο θεωρήματα στα οποία αναφέρεται ο G. H. Hardy στο απόφθεγμα που αναγράφεται στην αρχή του βιβλίου.

κοινούς παράγοντες των α και β μπορούμε να θεωρήσουμε ότι ο α και ο β δεν έχουν κοινούς παράγοντες. Συνεπώς αν ο α είναι άρτιος (ή ο β είναι άρτιος) τότε ο β είναι περιττός (αντίστοιχα ο α είναι περιττός). Αλλά έχουμε $2\beta^2 = \alpha^2$ και συνεπώς ο α^2 είναι άρτιος. Άρα ο α είναι άρτιος (γιατί;), έστω $\alpha = 2\kappa$. Οπότε $\beta^2 = 2\kappa^2$, δηλαδή και ο β είναι άρτιος που είναι άτοπο σύμφωνα με την υπόθεση.

Άλλοι γνωστοί άρρητοι αριθμοί είναι ο $\pi(= 3,14159\cdots)$ και ο $e(= 2,71828\cdots)$.

Μια σύντομη απόδειξη ότι ο e είναι άρρητος είναι η εξής (οι γνωστές αποδείξεις για το π είναι περισσότερο πολύπλοκες). Ο e ορίζεται ως

$$e = \sum_{n=1}^{\infty} \frac{1}{n!}.$$

Υποθέτουμε ότι $e = \dfrac{\alpha}{\beta}$, όπου α και β είναι ακέραιοι που δεν έχουν κοινούς παράγοντες. Έστω

$$p = 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{\beta!} \quad \text{και} \quad q = \frac{1}{(\beta+1)!} + \frac{1}{(\beta+2)!} + \cdots$$

οπότε $e = p + q$ και $\beta!e = \beta!p + \beta!q$. Οι αριθμοί $\beta!e$ και $\beta!p$ είναι ακέραιοι και συνεπώς και ο $\beta!q = \beta!e - \beta!p$ είναι ακέραιος. Αλλά έχουμε

$$\begin{aligned} 0 < \beta!q &= \frac{1}{\beta+1} + \frac{1}{(\beta+1)(\beta+2)} + \frac{1}{(\beta+1)(\beta+2)(\beta+3)} + \cdots \\ &< \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 1 \end{aligned}$$

(γεωμετρική πρόοδος). Αυτό είναι άτοπο, αφού δεν υπάρχει ακέραιος μεταξύ του 0 και του 1. Συνεπώς ο e είναι άρρητος.

4. Δείχνουμε ότι η διαφορά των τετραγώνων δύο περιττών αριθμών είναι πάντα ένα πολλαπλάσιο του 8.

Έστω $\alpha = 2k + 1$ ένας περιττός. Αν $k = 2k_1$, τότε $\alpha = 4k_1 + 1$ και αν $k = 2k_1 + 1$, τότε $\alpha = 4k_1 + 3 = 4(k_1 + 1) - 1$. Άρα και στις δύο περιπτώσεις το α^2 είναι της μορφής $8\pi + 1$, $\pi \in \mathbb{Z}$. Οπότε αν β είναι ένας άλλος περιττός, τότε $\alpha^2 - \beta^2 = 8\lambda$, $\lambda \in \mathbb{Z}$.

5. Μια πολύ απλή αλλά χρήσιμη μέθοδο για τη λύση προβλημάτων είναι η ***αρχή των περιστερώνων***. Αυτή αναφέρει ότι αν n αντικείμενα τοποθετηθούν σε k κιβώτια και είναι $k < n$, τότε τουλάχιστον

ένα κιβώτιο θα περιέχει περισσότερα από ένα αντικείμενα. Εφαρμόζοντας αυτή την αρχή μπορούμε να δείξουμε ότι μεταξύ $n+1$ ακεραίων αριθμών υπάρχουν δύο που η διαφορά τους διαιρείται δια του n. Πράγματι, έστω $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{n+1}$ οι $n+1$ αριθμοί και έστω

$$\alpha_i = n\pi_i + \upsilon_i, \quad 0 \leq \upsilon_i < n$$

οι $n+1$ Ευκλείδειες διαιρέσεις των α_i δια του n. Κάθε υπόλοιπο υ_i είναι ίσο με έναν απ' τους n αριθμούς $0, 1, 2, \ldots, n-1$. Επειδή έχουμε $n+1$ υπόλοιπα, απ' την αρχή των περιστερώνων, δύο απ' αυτά πρέπει να είναι ίσα, έστω $\upsilon_j = \upsilon_k$. Οπότε $\alpha_j - \alpha_k = n(\pi_j - \pi_k)$.

6. Το τελευταίο ψηφίο του τετραγώνου ενός ακεραίου αριθμού είναι ένας από τους αριθμούς $0, 1, 4, 5, 6$ ή 9.

Πράγματι, κάθε ακέραιος α γράφεται ως $\alpha = 10\pi + \upsilon$, $0 \leq \upsilon \leq 9$, όπου το υ είναι το τελευταίο ψηφίο του α. Έχουμε $\alpha^2 = 100\pi^2 + 20\pi\upsilon + \upsilon^2$. Συνεπώς το τελευταίο ψηφίο του α^2 είναι το ίδιο με το τελευταίο ψηφίο του υ^2. Αλλά το τετράγωνο των αριθμών $0, 1, 2, 3, \ldots, 9$ έχουν τελευταίο ψηφίο έναν απ' τους αριθμούς $0, 1, 4, 5, 6$ ή 9. Συνεπώς το τελευταίο ψηφίο ενός τέλειου τετραγώνου πρέπει να είναι $0, 1, 4, 5, 6$ ή 9. Φυσικά το αντίστροφο δεν ισχύει, π.χ. ο 5 δεν είναι τέλειο τετράγωνο.

Απ' τα μαθητικά μας χρόνια έχουμε μάθει να γράφουμε τους ακέραιους αριθμούς στο λεγόμενο "δεκαδικό σύστημα", π.χ. ο αριθμός 319 παριστά τον $3 \cdot 10^2 + 1 \cdot 10 + 9$. Η παράσταση αυτή των ακεραίων είναι μια ειδική περίπτωση του επόμενου θεωρήματος που προκύπτει ως μια εφαρμογή της Ευκλείδειας διαίρεσης.

1.2.10 Θεώρημα. (**β-αδική παράσταση ακεραίων**). *Έστω $\beta > 1$ ένας φυσικός αριθμός. Κάθε θετικός ακέραιος αριθμός α μπορεί να παρασταθεί μοναδικά με τη μορφή*

$$\alpha = \alpha_m \beta^m + \alpha_{m-1}\beta^{m-1} + \cdots + \alpha_1\beta + \alpha_0 \tag{1}$$

όπου m είναι ένας φυσικός αριθμός και τα α_i είναι ακέραιοι, τέτοιοι ώστε

$$0 \leq \alpha_i \leq \beta - 1, \quad i = 0, 1, 2, \ldots, m \quad \textit{και} \quad \alpha_m \neq 0.$$

Απόδειξη. Κατ' αρχάς δείχνουμε ότι ο α μπορεί να παρασταθεί με τη μορφή (1). Θεωρούμε τις Ευκλείδειες διαιρέσεις:

$$\begin{aligned}
\alpha = \pi_0 &= \beta\pi_1 + \alpha_0, \quad 0 \le \alpha_0 < \beta, \quad \pi_1 \ge 0. \quad \text{Αν} \quad \pi_1 \ge \beta \\
\pi_1 &= \beta\pi_2 + \alpha_1, \quad 0 \le \alpha_1 < \beta, \quad \pi_2 \ge 0. \quad \text{Αν} \quad \pi_2 \ge \beta \\
\pi_2 &= \beta\pi_3 + \alpha_2, \quad 0 \le \alpha_2 < \beta, \quad \pi_3 \ge 0. \quad \text{Αν} \quad \pi_3 \ge \beta
\end{aligned}$$

ξαναδιαιρούμε και συνεχίζοντας με τον ίδιο τρόπο σχηματίζεται η αυστηρά φθίνουσα ακολουθία $\pi_0 = \alpha > \pi_1 > \pi_2 > \cdots \ge 0$. Απ' την αρχή του ελαχίστου το σύνολο $\{\alpha, \pi_1, \pi_2, \ldots\}$ έχει ένα ελάχιστο στοιχείο έστω το π_m. Τότε το π_{m+1} δεν μπορεί να είναι ένας φυσικός αριθμός και άρα $\pi_{m+1} = 0$. Έτσι απ' τις διαιρέσεις $\pi_{i-1} = \beta\pi_i + \alpha_{i-1}$, $i = 0, \ldots, m$, με διαδοχικές αντικαταστάσεις των π_i παίρνουμε

$$\begin{aligned}
&\alpha = \beta\pi_1 + \alpha_0 = \beta(\beta\pi_2 + \alpha_1) + \alpha_0 = \beta(\beta\pi_3 + \alpha_2) + \beta\alpha_1 + \alpha_0 \\
&= \cdots = \alpha_m\beta^m + \alpha_{m-1}\beta^{m-1} + \cdots + \alpha_1\beta + \alpha_0 \quad \text{όπου} \quad \alpha_m = \pi_m \ne 0.
\end{aligned}$$

Αποδεικνύουμε τώρα τη μοναδικότητα της (1).

Έστω ότι ο α έχει την παράσταση (1) όπως στο θεώρημα. Έστω $k \in \{0, 1, \ldots, m-1\}$. Τότε έχουμε

$$\frac{\alpha}{\beta^k} = \alpha_m\beta^{m-k} + \cdots + \alpha_k + \frac{\alpha_{k-1}}{\beta} + \frac{\alpha_{k-2}}{\beta^2} + \cdots + \frac{\alpha_0}{\beta^k}. \tag{2}$$

Αλλά, επειδή $0 \le \alpha_i \le \beta - 1$, $i = 1, \ldots, m$, εφαρμόζοντας την ισότητα $\dfrac{x^{n+1}-1}{x-1} = x^n + \cdots + x + 1$, έχουμε

$$\begin{aligned}
0 \le \frac{\alpha_{k-1}}{\beta} + \frac{\alpha_{k-2}}{\beta^2} + \cdots + \frac{\alpha_0}{\beta^k} &\le \frac{\beta-1}{\beta} + \frac{\beta-1}{\beta^2} + \cdots + \frac{\beta-1}{\beta^k} \\
&= (\beta-1)\left(\frac{\frac{1}{\beta^{k+1}} - 1}{\frac{1}{\beta} - 1}\right) \\
&= 1 - \frac{1}{\beta^k}.
\end{aligned}$$

Έτσι το ακέραιο μέρος του $\dfrac{\alpha}{\beta^k}$ και του $\dfrac{\alpha}{\beta^{k+1}}$ ισούται αντίστοιχα με

$$\left[\frac{\alpha}{\beta^k}\right] = \alpha_m\beta^{m-k} + \cdots + \alpha_k \quad \text{και} \quad \left[\frac{\alpha}{\beta^{k+1}}\right] = \alpha_m\beta^{m-k-1} + \cdots + \alpha_{k+1},$$

οπότε $\alpha_k = \left[\frac{\alpha}{\beta^k}\right] - \beta\left[\frac{\alpha}{\beta^{k+1}}\right]$, $k \in \{0, 1, \ldots, m\}$.

Λόγω της (1), ισχύει $\beta^m \leq \alpha$ και καθώς $0 \leq \alpha_i \leq \beta - 1$, ισχύει $\alpha = \alpha_m\beta^m + \cdots + \alpha_0 \leq (\beta-1)(\beta^m + \cdots + 1) = \beta^{m+1} - 1 < \beta^{m+1}$. Δηλαδή $\beta^m \leq \alpha < \beta^{m+1}$. Συνεπώς, $m \log\beta \leq \log\alpha < (m+1)\log\beta$ και άρα $m \leq \dfrac{\log\alpha}{\log\beta} < m+1$. Αυτό μας λέει ότι ο m είναι το ακέραιο μέρος του πραγματικού αριθμού $\dfrac{\log\alpha}{\log\beta}$. Συνεπώς αν υπάρχει μια παράσταση του α, όπως αυτή που αναφέρεται στο θεώρημα, οι συντελεστές α_i και ο φυσικός αριθμός m καθορίζονται μοναδικά από τον α. □

Σημειώνουμε ότι ο G. E. Andreus [2] έχει αποδείξει το θεώρημα χρησιμοποιώντας επιχειρήματα που δίνουν ταυτόχρονα την ύπαρξη και μοναδικότητα χωρίς να εφαρμόζει την Ευκλείδεια διαίρεση. Στον Andrews η απόδειξη του θεωρήματος της Ευκλείδειας διαίρεσης στηρίζεται στην β-αδική παράσταση ενός θετικού ακεραίου. Εδώ η απόδειξη της μοναδικότητας είναι αυτή όπως αναφέρεται στον W. Sierpinski [16]. Η απόδειξη της ύπαρξης εδώ μας προσφέρει μια κατασκευαστική μέθοδο για την εύρεση της β-αδικής παράστασης του α. Για παράδειγμα, για την 5-αδική παράσταση του $\alpha = 15653$ εκτελούμε τις διαιρέσεις: $15653 = 5 \cdot 3130 + 3$, $3130 = 5 \cdot 626 + 0$, $626 = 5 \cdot 125 + 1$ $125 = 5 \cdot 25 = 0$, $25 = 5 \cdot 5 + 0$, $5 = 5 \cdot 1$, οπότε $m = 6$, $\alpha_6 = 1$, $\alpha_5 = 0$, $\alpha_4 = 0$, $\alpha_3 = 0$, $\alpha_2 = 1$, $\alpha_1 = 0$, $\alpha_0 = 3$, δηλαδή ο $\alpha = 15653$ σε 5-αδική παράσταση γράφεται ως 1000103.

Συνήθως για την β-αδική παράσταση του $\alpha = \sum_{i=0}^{m} \alpha_i\beta^i$ γράφουμε $\alpha = (\alpha_m\alpha_{m-1}\ldots\alpha_0)_\beta$, π.χ. γράφουμε

$$(15653)_{10} = (1000103)_5 = (1100111110101)_2.$$

Επίσης τους φυσικούς αριθμούς α_i τους ονομάζουμε ***ψηφία της παράστασης*** και τον αριθμό β ***βάση της παράστασης***. Προσθέτουμε, αφαιρούμε, πολλαπλασιάζουμε και διαιρούμε δύο αριθμούς σε β-αδική παράσταση ακολουθώντας τους ίδιους κανόνες με εκείνους που εφαρμόζουμε όταν εκτελούμε αυτές τις πράξεις στη δεκαδική παράσταση των αριθμών.

Για παράδειγμα, έστω $\beta = 5$, $\alpha = (123)_5$, $\alpha' = (43)_5$, οπότε $\alpha =$

$(38)_{10}$ και $\alpha' = (23)_{10}$. Έχουμε

$$\begin{array}{r} (123)_5 \\ +(43)_5 \\ \hline (221)_5 \end{array} \qquad \begin{array}{r} (123)_5 \\ -(43)_5 \\ \hline (30)_5 \end{array} \qquad \begin{array}{r} (123)_5 \\ \times(43)_5 \\ \hline 424)_5 \\ (1102)_5 \\ \hline (11444)_5 \end{array} \qquad \begin{array}{r|l} (123)_5 & (43)_5 \\ -(43)_5 & 1 \\ \hline (030)_5 & \end{array}$$

Για να αποφεύγουμε τυχόν λάθη, όταν εκτελούμε αυτές τις πράξεις, είναι χρήσιμο να γνωρίζουμε τους πίνακες της πρόσθεσης και του πολλαπλασιασμού για τους αριθμούς που είναι μικρότεροι της βάσης β. Για παράδειγμα, στο δεκαδικό σύστημα αυτοί οι πίνακες είναι η γνωστή προπαίδεια που διδάσκεται στα πρώτα χρόνια του δημοτικού σχολείου. Για $\beta = 2$, $\beta = 3$ και $\beta = 5$ έχουμε τους εξής πίνακες

$\beta = 2$

$+$	0	1
0	0	1
1	1	10

$\times$	0	1
0	0	0
1	0	1

$\beta = 3$

$+$	0	1	2
0	0	1	2
1	1	2	10
2	2	10	11

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	11

$\beta = 5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

Ιδιαιτέρως για τον καθορισμό της 2-αδικής παράστασης ενός αριθμού θεωρούμε τον ίδιο τον αριθμό και τα διαδοχικά πηλίκα π_i. Παραδείγματος χάριν, για $\alpha = 3125$ έχουμε τους αριθμούς 3125, 1562, 781, 390, 195, 97, 48, 24, 12, 6, 3,1. Καθένας απ' αυτούς τους αριθμούς είναι το $\frac{1}{2}$ του προηγούμενου παραλείποντας το υπόλοιπο. Δηλαδή έχουμε $\pi_i = \dfrac{\pi_{i-1} - \alpha_i}{2}$,

$i = 1, 2, \ldots, m$. Με αυτό τον τρόπο παίρνουμε τα ψηφία σε αντίστροφη διάταξη γράφοντας για κάθε αριθμό, 0 ή 1 αν ο αριθμός είναι άρτιος ή περιττός αντίστοιχα. Για παράδειγμα, για τον $\alpha = 3125$ έχουμε

$$(3125)_{10} = (110000110101)_2.$$

Αυτή η μέθοδος οδηγεί στον εξής ασυνήθιστο πολλαπλασιασμό δύο αριθμών α και α' και είναι γνωστός ως ο ***πολλαπλασιασμός των Ρώσων Αγροτών***: Σχηματίζουμε δύο στήλες αριθμών.

Η πρώτη αποτελείται από τους αριθμούς ξεκινώντας από τον α, καθένας των οποίων είναι το $\frac{1}{2}$ του προηγούμενου παραλείποντας το υπόλοιπο.

Η δεύτερη αποτελείται από τους αριθμούς, καθένας των οποίων είναι ο διπλάσιος του προηγούμενού του ξεκινώντας από τον α'. Αν στη δεύτερη στήλη διαγράψουμε τους αριθμούς που αντιστοιχούν σε άρτιους αριθμούς της πρώτης στήλης, τότε το άθροισμα αυτών που μένουν είναι το ζητούμενο γινόμενο $\alpha \cdot \alpha'$. Για παράδειγμα, έστω $\alpha = 36$ και $\alpha' = 11$, έχουμε

$$\begin{array}{rr} 36 & 11 \\ 18 & \cancel{22} \\ 9 & 44 \\ 4 & \cancel{88} \\ 2 & \cancel{176} \\ 1 & 352 \\ \hline & 396 \end{array} = 36 \cdot 11$$

Η μέθοδος αυτή στηρίζεται στο γεγονός ότι

$$\alpha \cdot \alpha' = \left(\sum_{i=0}^{m} \alpha_i 2^i \right) \alpha' = \sum_{\alpha_j^j = 1} 2^j \alpha'$$

$$36 \cdot 11 = (2^5 + 2^2) \cdot 11 = 352 + 44 = 396.$$

Περιγράφουμε τώρα ένα παιχνίδι που αναφέρεται σε κάρτες και στηρίζεται στο 2-αδικό σύστημα αριθμών. Θεωρούμε τους $2^n - 1$ αριθμούς, $n \in \mathbb{N}$, απ' το 1 έως το $2^n - 1$. Τους γράφουμε στην δεκαδική και στη 2-αδική

τους μορφή. Επίσης θεωρούμε n κάρτες $A_0, A_1, \ldots, A_{n-1}$, έτσι ώστε η A_i κάρτα να περιέχει όλους τους αριθμούς της μορφής

$$(\alpha_{n-1}\alpha_{n-2}\ldots(\alpha_i = 1)\ldots\alpha_1\alpha_0)_2$$

δηλαδή τους αριθμούς που το i-οστό ψηφίο α_i στην 2-αδική παράσταση είναι ίσο με 1. Άρα το πλήθος των αριθμών που περιέχει κάθε κάρτα είναι 2^{n-1}. Αν επιλέξουμε έναν αριθμό α μεταξύ των αριθμών 1 έως $2^n - 1$ που περιέχεται στις κάρτες $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$, τότε ο αριθμός α πρέπει να είναι το άθροισμα

$$2^{i_1} + 2^{i_2} + \cdots + 2^{i_k}.$$

Πράγματι, ο αριθμός $2^{i_j} = (0, 0\ldots010\ldots0)_2$ που έχει το 1 στη θέση i_j και όλα τα άλλα ψηφία του είναι 0 περιέχεται μόνο στην κάρτα A_{i_j} και καθώς ο α περιέχεται στις κάρτες A_{i_j}, $j = 1, \ldots, k$, ο α θα έχει ως μη-μηδενικά ψηφία μόνο τα α_{i_j}, $j = 1, \ldots, k$, δηλαδή θα είναι

$$\alpha = (0\ldots\alpha_{i_1}\ldots0\alpha_{i_2}0\ldots\alpha_{i_k}\ldots0)_2 = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_k}.$$

Για παράδειγμα, αν $n = 5$ τότε έχουμε 5 κάρτες A_1, A_2, A_3, A_4 και A_5 τέτοιες ώστε οι αριθμοί απ' το 1 έως το 31 κατανέμονται ως εξής

$$A_1 : 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31$$

$$A_2 : 2, 3, 6, 7, 10, 11, 14, 15, 18, 19, 22, 23, 26, 27, 30, 31$$

$$A_3 : 4, 5, 6, 7, 12, 13, 14, 15, 20, 21, 22, 23, 28, 29, 30, 31$$

$$A_4 : 8, 9, 10, 11, 12, 13, 14, 15, 24, 25, 26, 27, 28, 29, 30, 31$$

$$A_5 : 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31.$$

Η Σοφία ζητάει από την Πελαγία να επιλέξει έναν αριθμό απ' το 1 έως το 31 χωρίς να τον αποκαλύψει αλλά να αναφέρει σε ποιές κάρτες βρίσκεται αυτός ο αριθμός. Η Πελαγία αναφέρει ότι ο αριθμός που επέλεξε περιέχεται στις κάρτες $A_1, A_2.A_4$ και A_5. Τότε η Σοφία γνωρίζει ότι ο αριθμός αυτός πρέπει να είναι ο 27, γιατί

$$1 + 2 + 8 + 16 = 27.$$

1.3 Μέγιστος Κοινός Διαιρέτης και Ελάχιστο Κοινό Πολλαπλάσιο

Απ' την ιδιότητα 1.2.3 ix) προκύπτει ότι το πλήθος των διαιρετών ενός $\neq 0$ ακεραίου αριθμού είναι πεπερασμένο. Συνεπώς το πλήθος των κοινών διαιρετών δύο ακεραίων αριθμών α και β (ή και περισσοτέρων των δύο), που τουλάχιστον ένας απ' αυτούς είναι διάφορος του μηδενός, είναι πεπερασμένο και ≥ 1, αφού το 1 είναι ένας κοινός διαιρέτης. Άρα, λόγω της "ολικής διάταξης" των ακεραίων, υπάρχει ένας μοναδικός μέγιστος κοινός διαιρέτης των α και β που είναι μεγαλύτερος ή ίσος του 1.

1.3.1 Ορισμός. *Έστω $\alpha, \beta \in \mathbb{Z}$ έτσι ώστε $\alpha^2 + \beta^2 \neq 0$.*[5] ***Ο μέγιστος κοινος διαιρέτης*** *(μ.κ.δ.) των α και β, που θα συμβολίζεται* ***μ.κ.δ.(α, β)*** *ή απλά* ***(α, β)****, είναι ο θετικός ακέραιος δ που ικανοποιεί τις δύο ιδιότητες:*

i) $\delta \mid \alpha$ *και* $\delta \mid \beta$

ii) αν $\gamma \mid \alpha$ *και* $\gamma \mid \beta$ *τότε* $\gamma \leq \delta$.

☞ **Παραδείγματα. 1.** Οι αριθμοί $\pm 1, \pm 2, \pm 7$ και ± 14 είναι οι διαιρέτες του 14, ενώ οι $\pm 1, \pm 5, \pm 7$ και ± 35 είναι οι διαιρέτες του -35. Συνεπώς οι κοινοί διαιρέτες του 14 και -35 είναι οι ± 1 και ± 7. Άρα μ.κ.δ.$(14, -35) = 7$.

2. Ας θεωρήσουμε τους θετικούς κοινούς διαιρέτες δ των $n^2 + 1$ και $(n+1)^2 + 1$, $n \in \mathbb{N}$. Έστω $\delta \mid n^2 + 1$ και $\delta \mid n^2 + 2n + 2$, οπότε απ' την 1.2.3 viii) έχουμε $\delta \mid n^2 + 2n + 2 - (n^2 + 1) = 2n + 1$. Άρα $\delta \mid (2n+1)^2 = 4n^2+4n+1$, οπότε $\delta \mid 4(n^2+2n+2)-(4n^2+4n+1) = 4n+7$. Οπότε $\delta \mid 4n + 7 - 2(2n + 1) = 5$. Δηλαδή ο δ μπορεί να είναι ο 1 ή ο 5. Αν $n = 5k, 5k + 1, 5k + 3$ ή $5x + 4$, τότε προκύπτει ότι ο δ είναι ο 1. Αν $\delta = 5k + 2$ τότε ο δ είναι ο 1 και ο 5. Οπότε

$$\text{μ.κ.δ.}(n^2 + 1, (n + 1)^2 + 1) = \begin{cases} 1 & \text{αν} \quad n = 5k + \upsilon, \quad \upsilon = 0, 1, 3, \text{ ή } 5 \\ 5 & \text{αν} \quad n = 5k + 2. \end{cases}$$

[5] Προφανώς $\alpha^2 + \beta^2 \neq 0$ αν και μόνον αν $\alpha \neq 0$ ή $\beta \neq 0$.

Τώρα ας θεωρήσουμε όλα τα κοινά πολλαπλάσια δύο ακεραίων αριθμών α και β που και οι δύο[6] είναι $\neq 0$. Τέτοια υπάρχουν, για παράδειγμα οι αριθμοί $\alpha\beta k$, $k \in \mathbb{Z}$. Από την αρχή του ελάχιστου, υπάρχει ένα ελάχιστο κοινό πολλαπλάσιο των α και β στο σύνολο όλων των θετικών κοινών πολλαπλάσιων των α και β (που είναι $\neq \emptyset$ αφού ο $|\alpha|\,|\beta|$ είναι ένα τέτοιο).

1.3.2 Ορισμός. *Το* ***ελάχιστο κοινό πολλαπλάσιο*** *των α και β, $\alpha, \beta \in \mathbb{Z}$, $\alpha \neq 0$, $\beta \neq 0$, είναι ο θετικός ακέραιος ε που συμβολίζεται με* $[\boldsymbol{\alpha}, \boldsymbol{\beta}]$ *και ικανοποιεί τις εξής ιδιότητες.*

i) $\alpha \mid \varepsilon$ *και* $\beta \mid \varepsilon$

ii) αν $\alpha \mid m$ *και* $\beta \mid m$ *τότε* $\varepsilon \leq m$.

Για παράδειγμα, $[5, -15] = 15$, $[5, 21] = 105$.

1.3.3 Θεώρημα. *i) Τα κοινά πολλαπλάσια δύο ακέραιων αριθμών $\alpha \neq 0$, $\beta \neq 0$, είναι τα ίδια με τα πολλαπλάσια του $[\alpha, \beta]$.*

ii) Ένας κοινός διαιρέτης δύο αριθμών $\alpha, \beta \in \mathbb{Z}$, με $\alpha^2 + \beta^2 \neq 0$, είναι ο μ.κ.δ.$(\alpha, \beta)$ αν και μόνον αν αυτός διαιρείται με κάθε κοινό διαιρέτη των α και β. Δηλαδή οι κοινοί διαιρέτες των α και β είναι ακριβώς εκείνοι του μ.κ.δ.$(\alpha, \beta) = (\alpha, \beta)$.

Απόδειξη. i) Έστω $\varepsilon = [\alpha, \beta]$ και m ένα κοινό πολλαπλάσιο των α και β. Από την Ευκλείδεια διαίρεση υπάρχουν μοναδικοί π, $\upsilon \in \mathbb{Z}$ με $0 \leq \upsilon < \varepsilon$ τέτοιοι ώστε

$$m = \varepsilon\pi + \upsilon.$$

Άρα $\upsilon = m - \varepsilon\pi$ και συνεπώς $\alpha \mid \upsilon$ και $\beta \mid \upsilon$. Αν ήταν $\upsilon \neq 0$, τότε θα υπήρχε ένα θετικό κοινό πολλαπλάσιο των α και β που είναι μικρότερο του ε. Συνεπώς θα πρέπει $\upsilon = 0$ δηλαδή, $\varepsilon \mid m$.

ii) Αν $\alpha = 0$ και $\beta \neq 0$, τότε $(0, \beta) = |\beta|$. Οπότε αν $\gamma \mid \beta$ (και $\gamma \mid 0$) τότε $\gamma \mid (0, \beta)$. Αν $\alpha \neq 0$ και $\beta \neq 0$, μπορούμε να υποθέσουμε ότι $\alpha > 0$ και $\beta > 0$, αφού ο α έχει τους ίδιους διαιρέτες με τον $|\alpha|$ και το ίδιο ισχύει για τον β. Απ' την i) γνωρίζουμε ότι $\varepsilon \mid \alpha\beta$, αφού ο $\alpha\beta$ είναι κοινό πολλαπλάσιο των α και β. Δηλαδή υπάρχει $\delta \in \mathbb{Z}$ τέτοιο ώστε

$$\alpha\beta = \varepsilon\delta.$$

[6] Αν ένας τουλάχιστον είναι $= 0$ τότε τα κοινά πολλαπλάσια είναι μόνο το 0.

Θα δείξουμε ότι αν $\gamma \mid \alpha$ και $\gamma \mid \beta$ τότε $\gamma \mid \delta$ και ότι $\delta = (\alpha, \beta)$. Προφανώς ισχύει

$$\alpha \mid \alpha\frac{\beta}{\gamma} \quad \text{και} \quad \beta \mid \beta\frac{\alpha}{\gamma},$$

δηλαδή ο $\dfrac{\alpha\beta}{\gamma}$ είναι ένα κοινό πολλαπλάσιο των α και β. Συνεπώς, απ' την i), πρέπει $\varepsilon \Big| \dfrac{\alpha\beta}{\gamma}$. Δηλαδή το κλάσμα

$$\frac{\alpha\beta}{\gamma} \Big/ \frac{\alpha\beta}{\delta} = \frac{\delta}{\gamma} \in \mathbb{Z},$$

δηλαδή $\gamma \mid \delta$ (άρα $\gamma \leq \delta$). Επίσης ισχύει $\dfrac{\alpha}{\delta} = \dfrac{\varepsilon}{\beta} \in \mathbb{Z}$ και $\dfrac{\beta}{\delta} = \dfrac{\varepsilon}{\alpha} \in \mathbb{Z}$, που σημαίνει ότι $\delta \mid \alpha$ και $\delta \mid \beta$. Άρα ο δ είναι ο μεγαλύτερος κοινός διαιρέτης των α και β, δηλαδή $\delta = (\alpha, \beta)$. Το αντίστροφο είναι προφανές. □

1.3.4 Πόρισμα. *Αν $\alpha, \beta \in \mathbb{Z}$ με $\alpha^2 + \beta^2 \neq 0$, τότε*

$$[\alpha, \beta] = \frac{|\alpha|\,|\beta|}{(\alpha, \beta)}.$$

Απόδειξη. Αυτό έχει δειχθεί στην απόδειξη του 1.3.3 ii). □

1.3.5 Παρατήρηση. Λόγω του Θεωρήματος 1.3.3, στον Ορισμό 1.3.1 (και αντίστοιχα 1.3.2) θα μπορούσαμε να αντικαταστήσουμε την ανισότητα $\gamma \leq \delta$ στην ιδιότητα ii. με την διαιρετότητα $\gamma \mid \delta$ (αντίστοιχα την ανισότητα $\varepsilon \leq m$ με την $\varepsilon \mid m$). Σ' αυτή την περίπτωση, δηλαδή αν κάνουμε αυτή την αντικατάσταση, τότε η ύπαρξη του μ.κ.δ. (και συνεπώς του ε.κ.π.) εξασφαλίζεται από το επόμενο Θεώρημα 1.3.6 ή τον Ευκλείδειο Αλγόριθμο που θα αναφερθεί πιο κάτω. Σημειώνουμε οτι σε πολλά αλγεβρικά συστήματα (για παράδειγμα στους πολυωνυμικούς δακτυλίους) όπου υπάρχει η έννοια του μ.κ.δ. αυτός γενικά ορίζεται μ' αυτόν το τρόπο, δηλαδή η ανισότητα στον Ορισμό 1.3.1 αντικαθίσταται με τη διαιρετότητα.

Μία σημαντική ιδιότητα που χαρακτηρίζει τον μ.κ.δ.(α, β) και χρησιμοποιείται συχνά για τη λύση προβλημάτων είναι η εξής.

1.3.6 Θεώρημα. (Γραμμική Μορφή του μ.κ.δ. η Θεώρημα Bachet - Bezout). *Έστω $\alpha, \beta \in \mathbb{Z}$ με $\alpha^2 + \beta^2 \neq 0$. Ο ακέραιος αριθμός δ είναι*

ο μ.κ.δ.(α,β) *αν και μόνον αν ο* δ *είναι ο μικρότερος θετικός ακέραιος μεταξύ όλων των θετικών αριθμών που μπορούν να εκφρασθούν στη γραμμική μορφή*

$$\alpha x+\beta y, \quad x,y\in\mathbb{Z}.$$

Δηλαδή οι αριθμοί της μορφής $\alpha x+\beta y$, $x,y\in\mathbb{Z}$ *είναι τα πολλαπλάσια του μ.κ.δ.*(α,β).

Απόδειξη. Έστω γ ο μικρότερος θετικός ακέραιος μεταξύ όλων των θετικών ακεραίων της μορφής $\alpha x+\beta y$, $x,y\in\mathbb{Z}$. Από την αρχή του ελάχιστου, τέτοιος γ υπάρχει αφού το σύνολο

$$\Sigma=\{\alpha x+\beta y\in\mathbb{N}-\{0\}/x,y\in\mathbb{Z}\}$$

είναι $\neq\emptyset$ (για παράδειγμα ο $|\alpha|\in\Sigma$, αν $\alpha\neq 0$). Έστω $\gamma=\alpha x_0+\beta y_0$. Διαιρώντας τον α δια του γ έχουμε

$$\alpha=\gamma\pi+\upsilon, \quad 0\leq\upsilon<\gamma.$$

Οπότε $\upsilon=\alpha-\gamma\pi=\alpha(1-x_0\pi)+\beta(-y_0\pi)$. Αν ήταν $\upsilon\neq 0$, τότε $\upsilon\in\Sigma$ που είναι άτοπο αφού $\upsilon<\gamma$. Συνεπώς πρέπει $\upsilon=0$. Άρα $\gamma\mid\alpha$. Όμοια προκύπτει ότι $\gamma\mid\beta$. Συνεπώς, απ΄το 1.3.3 ii) πρέπει $\gamma\mid(\alpha,\beta)=\delta$. Απ' τη γραμμική μορφή του γ, προκύπτει ότι και $(\alpha,\beta)\mid\gamma$ και άρα τελικά $\delta=(\alpha,\beta)=\gamma$.

Τώρα κάθε πολλαπλάσιο $\kappa\delta$ του δ είναι της μορφής $\alpha(kx_0)+\beta(ky_0)=\alpha x+\beta y$, $x,y\in\mathbb{Z}$, και φυσικά κάθε ακέραιος της μορφής $\alpha x+\beta y$ είναι πολλαπλάσιο του δ.

1.3.7 Παρατηρήσεις. i) Ο μ.κ.δ.(α,β) είναι ο μοναδικός θετικός κοινός διαιρέτης των α και β που μπορεί να γραφεί σε γραμμική μορφή $\alpha x+\beta y$, $x,y\in\mathbb{Z}$, αφού όλες αυτές οι εκφράσεις είναι πολλαπλάσια του $\delta=(\alpha,\beta)$.

ii) Αν $\alpha,\beta,x,y\in\mathbb{Z}$, τότε υπάρχουν άπειρα το πλήθος ζευγάρια (x',y'), $x',y'\in\mathbb{Z}$ τέτοια ώστε $\alpha x+\beta y=\alpha x'+\beta y'$. Πράγματι, αν γ είναι ένας κοινός διαιρέτης των α και β (π.χ. ο 1), έστω $\alpha=\alpha'\gamma$ και $\beta=\beta'\gamma$, οπότε $\dfrac{\alpha\beta}{\gamma}=\alpha'\beta=\alpha\beta'$. Έτσι έχουμε

$$\alpha x+\beta y=\alpha(x-\beta' t)+\beta(y+\alpha' t)=\alpha x'+\beta y', \quad t\in\mathbb{Z}$$

όπου $x'=x-\beta' t$ και $y'=y+\alpha' t$.

1.3.8 Ορισμός. *Έστω $\alpha, \beta \in \mathbb{Z}$ με $\alpha^2 + \beta^2 \neq 0$. Τότε λέμε ότι οι α και β είναι σχετικά πρώτοι μεταξύ τους ή ότι ο α είναι σχετικά πρώτος προς τον β, αν*

$$\mu.κ.δ.(\alpha, \beta) = 1,$$

δηλαδή αν οι μόνοι κοινοί διαιρέτες τους είναι ο 1 και ο -1.

Απ' το προηγούμενο θεώρημα, αν α και β είναι σχετικά πρώτοι μεταξύ τους, τότε υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $\alpha x + \beta y = 1$. Αντίστροφα, αν για δύο ακέραιους α και β υπάρχουν ακέραιοι x και y τέτοιοι ώστε $\alpha x + \beta y = 1$ τότε, επειδή $(\alpha, \beta) \mid 1$ και $(\alpha, \beta) > 0$, πρέπει $(\alpha, \beta) = 1$. Συνεπώς δύο σχετικά πρώτοι αριθμοί χαρακτηρίζονται ως εξής:

1.3.9 Πόρισμα. *Δύο ακέραιοι α και β που δεν είναι και οι δύο μηδέν, είναι σχετικά πρώτοι μεταξύ τους αν και μόνον αν υπάρχουν $x, y \in \mathbb{Z}$, τέτοιοι ώστε*

$$\alpha x + \beta y = 1.$$

☞ **Παράδειγμα.** Δείχνουμε ότι, για κάθε $n \in \mathbb{N}$, ισχύει

$$\text{μ.κ.δ.}(n! + 1, (n + 1)! + 1) = 1.$$

Πράγματι, έστω ότι για κάποιο $n \in \mathbb{N}$ ο μ.κ.δ. των $n! + 1$ και $(n + 1)! + 1$ είναι δ. Οπότε ο δ διαιρεί τον $(n + 1)(n! + 1) - ((n + 1)! + 1) = (n + 1)! + (n + 1) - (n + 1)! - 1 = n$, δηλαδή $\delta \mid n$. Άρα $\delta \mid \text{μ.κ.δ.}(n, n! + 1)$, αφού $\delta \mid n! + 1$. Αλλά $\text{μ.κ.δ.}(n, n! + 1) = 1$, αφού $1 = (n! + 1) \cdot 1 + n(-(n - 1)!)$. Συνεπώς $\delta = 1$.

Στην επόμενη πρόταση διατυπώνονται μερικές απλές αλλά βασικές ιδιότητες που αφορούν τον μ.κ.δ. και ε.κ.π. δύο ακεραίων αριθμών.

1.3.10 Πρόταση. **(*Βασικές ιδιότητες μ.κ.δ. και ε.κ.π.*).** *Έστω $\alpha, \beta, \gamma \in \mathbb{Z}$ με $\alpha^2 + \beta^2 \neq 0$. Τότε ισχύουν τα εξής:*

i) $(\alpha, \beta) = (|\alpha|, |\beta|)$ *και* $[\alpha, \beta] = [|\alpha|, |\beta|]$. *Ιδιαιτέρως ισχύει $\alpha \mid \beta$ αν και μόνον αν $(\alpha, \beta) = |\alpha|$ αν και μόνον αν $[\alpha, \beta] = |\beta|$. Επίσης $[\alpha, \beta] = (\alpha, \beta)$ αν και μόνον αν $|\alpha| = |\beta|$.*

ii) *Αν* $\gamma \neq 0$, *τότε* $(\gamma\alpha, \gamma\beta) = |\gamma|(\alpha, \beta)$. *Συνεπώς λόγω του 1.3.4 ισχύει* $[\gamma\alpha, \gamma\beta] = |\gamma|[\alpha, \beta]$.

iii) *Αν* $\gamma \mid (\alpha, \beta)$ *τότε* $\left(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}\right) = \frac{(\alpha, \beta)}{|\gamma|}$. *Ιδιαιτέρως ισχύει*

$$\left(\frac{\alpha}{(\alpha, \beta)}, \frac{\beta}{(\alpha, \beta)}\right) = 1.$$

iv) *Ισχύει* $(\alpha, \beta) = (\alpha + k\beta, \beta)$, *για κάθε* $k \in \mathbb{Z}$. *(Στην ιδιότητα αυτή στηρίζεται ο Ευκλείδειος αλγόριθμος που θα αναφερθεί πιο κάτω).*

v) **Το Λήμμα του Ευκλείδη.** *Αν* $\gamma \mid \alpha\beta$, *τότε* $\gamma \mid (\alpha, \gamma)(\beta, \gamma)$. *Απ' αυτό προκύπτει ότι,*

$$\text{αν} \quad \gamma \mid \alpha\beta, \quad \text{τότε} \quad \gamma \mid (\alpha, \gamma)\beta$$

και απ' αυτό προκύπτει ότι,

$$\text{αν} \quad \gamma \mid \alpha\beta \quad \text{και} \quad (\alpha, \gamma) = 1, \quad \text{τότε} \quad \gamma \mid \beta.$$

Συνεπώς, αν $\alpha m = \beta n$, *τότε* $\frac{\alpha}{(\alpha, \beta)} \Big| n$ *και* $\frac{\beta}{(\alpha, \beta)} \Big| m$.

Επίσης ισχύει $\gamma \mid \alpha\beta$ *αν και μόνον αν* $\frac{\gamma}{(\alpha, \gamma)} \Big| \beta$.

vi) *Ισχύει* $(\alpha, \beta\gamma) = (\alpha, (\alpha, \beta)\gamma)$. *Οπότε αν* $(\alpha, \beta) = 1$, *τότε* $(\alpha, \beta\gamma) = (\alpha, \gamma)$. *Συνεπώς* $(\alpha, \beta) = (\alpha, \gamma) = 1$ *αν και μόνον αν* $(\alpha, \beta\gamma) = 1$.

vii) *Αν* $(\alpha, \beta) = 1$ *και* $\gamma \mid \alpha$, *τότε* $(\beta, \gamma) = 1$.

viii) *Αν* $(\alpha, \beta) = 1$ *και* $\alpha \mid \gamma$, $\beta \mid \gamma$, *τότε* $\alpha\beta \mid \gamma$.

ix) *Αν* $(\alpha, \beta) = 1$, *τότε* $(\alpha\beta, \gamma) = (\alpha, \gamma)(\beta, \gamma)$ *και* $[\alpha\beta, \gamma] = [\alpha, \gamma][\beta, \gamma]$.

x) *Αν* $(\alpha, \beta) = 1$ *και* $\gamma \mid \alpha\beta$ *με* $\gamma > 0$, *τότε υπάρχουν μοναδικοί ακέραιοι αριθμοί* γ_1, γ_2 *τέτοιοι ώστε* $\gamma = \gamma_1\gamma_2$ *και* $\gamma_1 \mid \alpha$, $\gamma_2 \mid \beta$. *Είναι δε* $\gamma_1 = (\alpha, \gamma)$ *και* $\gamma_2 = (\beta, \gamma)$.

Απόδειξη. i) Ο α και ο $-\alpha$ έχουν τους ίδιους κοινούς διαιρέτες αφού $\gamma \mid \alpha$ αν και μόνον αν $\gamma \mid -\alpha$. Συνεπώς ο α και ο $|\alpha|$ έχουν τους ίδιους κοινούς διαιρέτες αφού ο $|\alpha|$ είναι ίσος με α ή με $-\alpha$. (Το ίδιο ισχύει και για τον β). Άρα ο γ είναι ένας κοινός διαιρέτης των α και β αν και μόνον αν είναι κοινός διαιρέτης των $|\alpha|$ και $|\beta|$. Συνεπώς $(\alpha,\beta) = (|\alpha|,|\beta|)$.

Το ίδιο ισχύει και για τα κοινά πολλαπλάσια των α και β. Άρα $[\alpha,\beta] = [|\alpha|,|\beta|]$. Απ' τον ορισμό του μ.κ.δ. και του ε.κ.π., είναι φανερό ότι $\alpha \mid \beta$ αν και μόνον αν $(\alpha,\beta) = |\alpha|$ και αυτό ισχύει αν και μόνον αν $[\alpha,\beta] = |\beta|$.

Έστω τώρα ότι $(\alpha,\beta) = [\alpha,\beta]$. Αυτό σημαίνει ότι $\alpha \mid (\alpha,\beta)$ αλλά $(\alpha,\beta) \mid \alpha$. Συνεπώς $|\alpha| = (\alpha,\beta)$ και απ' το προηγούμενο προκύπτει $|\alpha||\beta|$. Για τον ίδιο λόγο ισχύτει ότι $|\beta||\alpha|$. Άρα $|\alpha| = |\beta|$. Το αντίστροφο είναι προφανές.

ii) Από το 1.3.6 υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $(\gamma\alpha,\gamma\beta) = \gamma\alpha x + \gamma\beta y = \gamma(\alpha x + \beta y)$. Πάλι απ' το 1.3.6 πρέπει $(\alpha,\beta) \mid \alpha x + \beta y$, όπότε $\gamma(\alpha,\beta) \mid \gamma(\alpha x + \beta y) = (\gamma\alpha,\gamma\beta)$ και συνεπώς $|\gamma|(\alpha,\beta)|(\alpha\gamma,\alpha\beta)$. Επίσης υπάρχουν $x', y' \in \mathbb{Z}$ τέτοιοι ώστε $(\alpha,\beta) = \alpha x' + \beta y'$ και άρα $|\gamma|(\alpha,\beta) = |\gamma|(\alpha x' + \beta y') = |\gamma|\alpha x' + |\gamma|\beta y'$. Συνεπώς, από το 1.3.6, $(\gamma\alpha,\gamma\beta)\,|\,|\gamma|(\alpha,\beta)$. Άρα $(\gamma\alpha,\gamma\beta) = |\gamma|(\alpha,\beta)$.

iii) Αφού $\gamma \mid (\alpha,\beta)$ τότε $\gamma \mid \alpha$ και $\gamma \mid \beta$. Απ' την ii) προκύπτει ότι $(\alpha,\beta) = \left(\gamma\frac{\alpha}{\gamma}, \gamma\frac{\beta}{\gamma}\right) = |\gamma|\left(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}\right)$ που είναι το ζητούμενο. Ιδιαιτέρως $(\alpha,\beta) = (\alpha,\beta)\left(\frac{\alpha}{(\alpha,\beta)}, \frac{\beta}{(\alpha,\beta)}\right)$, οπότε για $\gamma = (\alpha,\beta)$ παίρνουμε

$$\left(\frac{\alpha}{(\alpha,\beta)}, \frac{\beta}{(\alpha,\beta)}\right) = \frac{(\alpha,\beta)}{(\alpha,\beta)} = 1.$$

iv) Επειδή $(\alpha,\beta) \mid \alpha$ και $(\alpha,\beta) \mid k\beta$ έχουμε ότι $(\alpha,\beta) \mid \alpha + k\beta$. Άρα $(\alpha,\beta) \mid (\alpha + k\beta,\beta)$ (ή αρκεί να συμπεράνουμε ότι $(\alpha,\beta) \leq (\alpha + k\beta,\beta)$ όπως απαιτεί ο Ορισμός 1.3.1). Επίσης έχουμε $(\alpha + k\beta,\beta) \mid k\beta$ και

$(\alpha + k\beta, \beta) \mid \alpha + k\beta - k\beta = \alpha$. Άρα $(\alpha + k\beta, \beta) \mid (\alpha, \beta)$. Συνεπώς $(\alpha, \beta) = (\alpha + k\beta, \beta)$.

v) Έστω $(\alpha, \gamma) = \alpha x_1 + \gamma y_1$, $(\beta, \gamma) = \beta x_2 + \gamma y_2$, $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. Οπότε $(\alpha, \gamma)(\beta, \gamma) = \alpha\beta x_1 x_2 + \gamma(\alpha x_1 y_2 + \beta y_1 x_2 + \gamma y_1 y_2)$ και επειδή $\gamma \mid \alpha\beta$ έπεται ότι $\gamma \mid (\alpha, \gamma)(\beta, \gamma)$.

Έστω $\beta = (\beta, \gamma)t$ και $(\alpha, \gamma)(\beta, \gamma) = \gamma s$, $t, s \in \mathbb{Z}$. Οπότε $(\alpha, \gamma)\beta = \gamma st$, δηλαδή $\gamma \mid (\alpha, \gamma)\beta$. Αν $(\alpha, \gamma) = 1$, τότε $\gamma \mid \beta$.

Αν ισχύει $\alpha m = \beta n$, $m, n \in \mathbb{Z}$, τότε $\dfrac{\alpha}{(\alpha, \beta)} m = \dfrac{\beta}{(\alpha, \beta)} n$ και επειδή $\left(\dfrac{\alpha}{(\alpha, \beta)}, \dfrac{\beta}{(\alpha, \beta)}\right) = 1$, και $\dfrac{\alpha}{(\alpha, \beta)} \Big| \dfrac{\beta}{(\alpha, \beta)} n$, απ' το προηγούμενο πρέπει $\dfrac{\alpha}{(\alpha, \beta)} \Big| n$.

Αν $\dfrac{\gamma}{(\alpha, \gamma)} \Big| \beta$, δηλαδή $\beta = \dfrac{\gamma}{(\alpha, \gamma)} t$, $t \in \mathbb{Z}$, τότε $\gamma t = \beta(\alpha, \gamma) = \beta \dfrac{\alpha}{t}$ οπότε $\gamma t t' = \beta\alpha$, όπου $\alpha = (\alpha, \gamma)t'$, $t' \in \mathbb{Z}$. Δηλαδή $\gamma \mid \alpha\beta$. Το αντίστροφο έχει ήδη δειχθεί.

vi) Επειδή $(\alpha, (\alpha, \beta)\gamma) \mid (\alpha, \beta)|\gamma| = (\alpha\gamma, \beta\gamma)$ θα πρέπει $(\alpha, (\alpha, \beta)\gamma) \mid \beta\gamma$. Αλλά $(\alpha, (\alpha, \beta)\gamma) \mid \alpha$, οπότε $(\alpha, (\alpha, \beta)\gamma) \mid (\alpha, \beta\gamma)$. Έχουμε όμως
$(\alpha, \beta\gamma) \mid \alpha$, οπότε $(\alpha, \beta\gamma) \mid \alpha\gamma$ και $(\alpha, \beta\gamma) \mid \beta\gamma$.

Συνεπώς $(\alpha, \beta\gamma) \mid (\alpha\gamma, \beta\gamma) = (\alpha, \beta)|\gamma|$ και επειδή $(\alpha, \beta\gamma) \mid \alpha$ θα πρέπει $(\alpha, \beta\gamma) \mid (\alpha, (\alpha, \beta)\gamma)$.

vii) Επειδή $(\beta, \gamma) \mid \gamma$ και $\gamma \mid \alpha$ προκύπτει ότι $(\beta, \gamma) \mid \alpha$. Αλλά $(\beta, \gamma) \mid \beta$ οπότε $(\beta, \gamma) \mid (\alpha, \beta) = 1$. Άρα $(\beta, \gamma) = 1$.

viii) Πράγματι, υπάρχουν $x, y \in \mathbb{Z}$ έτσι ώστε $\alpha x + \beta y = 1$, οπότε $\gamma\alpha x + \gamma\beta y = \gamma$. Αλλά $\alpha \mid \alpha$ και από την υπόθεση $\beta \mid \gamma$, άρα $\alpha\beta \mid \alpha\gamma$. Για τον ίδιο λόγο $\alpha\beta \mid \beta\gamma$. Συνεπώς $\alpha\beta \mid \alpha\gamma x + \beta\gamma y = \gamma$. Αυτό προκύπτει επίσης άμεσα από το 1.3.4 iii) αφού $[\alpha, \beta] \mid \gamma$ και $[\alpha, \beta] = |\alpha|\,|\beta|$.

ix) Έστω $\delta = (\alpha\beta, \gamma)$ και $\delta' = (\alpha, \gamma)(\beta, \gamma)$. Επειδή $(\alpha, \beta) = 1$ προκύπτει ότι $((\alpha, \gamma), (\beta, \gamma)) = 1$. Οπότε απ' την viii) έχουμε $\delta' | \gamma$, αφού

$(\alpha,\gamma)|\gamma$ και $(\beta,\gamma)|\gamma$. Επίσης $\delta'|\alpha\beta$ άρα $\delta'|(\alpha\beta,\gamma)=\delta$. Τώρα, έστω $\alpha x_1+\gamma y_1=(\alpha,\gamma)$ και $\beta x_2+\gamma y_2=(\beta,\gamma)$, $x_1,x_2,y_1,y_2\in Z$. Οπότε $\delta'=(\alpha,\gamma)(\beta,\gamma)=\alpha\beta x_1x_2+\gamma(\alpha x_1y_2+\beta x_2y_1+\gamma y_1y_2)$. Αλλά $\delta\mid\alpha\beta$ και $\delta\mid\gamma$ οπότε $\delta\mid\delta'$. Άρα $\delta=\delta'$. Η σχέση με το ε.κ.π. προκύπτει απ' την προηγούμενη σχεση και το 1.3.4.

x) Απ' την ix) έχουμε $(\alpha\beta,\gamma)=(\alpha,\gamma)(\beta,\gamma)$ αλλά, επειδή $\gamma\mid\alpha\beta$ προκύπτει ότι $\gamma=|\gamma|=(\alpha\beta,\gamma)=\gamma_1\gamma_2$, όπου $\gamma_1=(\alpha,\gamma)$, $\gamma_2=(\beta,\gamma)$. Δείχνουμε τώρα τη μοναδικότητα. Έστω $\gamma_1',\gamma_2'\in\mathbb{Z}$ με $\gamma_1'\mid\alpha$, $\gamma_2'\mid\beta$ και $\gamma=\gamma_1'\gamma_2'$. Προφανώς $\gamma_1'\mid(\alpha,\gamma)$ και $\gamma_2'\mid(\beta,\gamma)$. Αν ήταν $\gamma_1'\neq(\alpha,\gamma)$, τότε $\gamma_1'<(\alpha,\gamma)$, οπότε θα είχαμε $\gamma=\gamma_1'\gamma_2'<(\alpha,\gamma)(\beta,\gamma)=\gamma$, άτοπο. Το ίδιο θα ήταν αν $\gamma_2'\neq(\beta,\gamma)$. Άρα πρέπει $\gamma_1'=(\alpha,\gamma)$ και $\gamma_2'=(\beta,\gamma)$.

☞ **1.3.11 Παραδείγματα και Εφαρμογές.** Το υπόλοιπο της Ευκλείδειας διαίρεσης του $[m,n]-1$ δια του m είναι $m-1$, όπου $m,n\in\mathbb{N}$. Πράγματι, ισχύει

$$[m,n]-1=m\left(\frac{n}{(m,n)}-1\right)+m-1.$$

2. Δείχνουμε το γνωστό θεώρημα του Πυθαγόρα: ο αριθμός $\sqrt{2}$ δεν είναι ρητός. Πράγματι, αν ήταν $\sqrt{2}=\dfrac{\alpha}{\beta}$, μπορούμε να υποθέσουμε ότι $(\alpha,\beta)=1$, διαφορετικά διαιρούμε αριθμητή και παρανομαστή δια του (α,β) και σύμφωνα με την ιδιότητα iii) παίρνουμε ανάγωγο κλάσμα. Οπότε έχουμε $\alpha x+\beta y=1$, για κάποια $x,y\in\mathbb{Z}$, και άρα $\sqrt{2}=\sqrt{2}\alpha x+\sqrt{2}\beta y=2\beta x+\alpha y$, δηλαδή $\sqrt{2}\in\mathbb{Z}$ που είναι άτοπο, αφού δεν υπάρχει ακέραιος που το τετράγωνό του είναι ίσο με 2.

3. Δείχνουμε ότι για κάθε $n\in\mathbb{N}$ και $\alpha,\beta\in\mathbb{Z}$ με $\alpha^2+\beta^2\neq0$, ισχύει

$$(\alpha,\beta)^n=(\alpha^n,\beta^n).$$

Κατ' αρχάς υποθέτουμε ότι $(\alpha,\beta)=1$, οπότε $(\alpha,\beta)^n=1$. Επαγωγικά εύκολα μπορούμε να δείξουμε τη γενίκευση της ιδιότητας vi). Δηλαδή, αν $\alpha,\alpha_1,\ldots,\alpha_k\in\mathbb{Z}$, τότε ισχύει $(\alpha,\alpha_i)=1$, $i=1,\ldots,k$, αν και μόνον αν ισχύει $(\alpha,\alpha_1\alpha_2\ldots\alpha_k)=1$. Εφαρμόζοντας αυτή τη γενίκευση στην

$(\alpha,\beta)=1$, n φορές για το α παίρνουμε ότι $(\alpha^n,\beta)=1$. Εφαρμόζοντας πάλι την ίδια γενίκευση στην $(\alpha^n,\beta)=1$, n φορές για το β παίρνουμε τελικά $(\alpha^n,\beta^n)=1$.

Έστω τώρα ότι $(\alpha,\beta)\neq 1$. Γνωρίζουμε απ' την ιδιότητα iii) ότι

$$\left(\frac{\alpha}{(\alpha,\beta)},\frac{\beta}{(\alpha,\beta)}\right)=1,$$

οπότε, λόγω του προηγούμενου αποτελέσματος έχουμε

$$\begin{aligned}\left(\frac{\alpha^n}{(\alpha,\beta)^n},\frac{\beta^n}{(\alpha,\beta)^n}\right)&=\left(\left(\frac{\alpha}{(\alpha,\beta)}\right)^n,\left(\frac{\beta}{(\alpha,\beta)}\right)^n\right)\\&=\left(\frac{\alpha}{(\alpha,\beta)},\frac{\beta}{(\alpha,\beta)}\right)^n=1.\end{aligned}$$

Τέλος, από την ιδιότητα ii) έχουμε

$$(\alpha,\beta)^n=(\alpha,\beta)^n\left(\frac{\alpha^n}{(\alpha,\beta)^n},\frac{\beta^n}{(\alpha,\beta)^n}\right)=(\alpha^n,\beta^n).$$

4. Προφανώς, αν $\alpha\mid\beta$ τότε $\alpha^n\mid\beta^n$, $\forall\, n\in\mathbb{N}$. Στηριζόμενοι στο προηγούμενο παράδειγμα δείχνουμε ότι ισχύει και το αντίστροφο, δηλαδή αν $\alpha^n\mid\beta^n$ τότε $\alpha\mid\beta$. Έστω $\alpha=\alpha_1(\alpha,\beta)$ και $\beta=\beta_1(\alpha,\beta)$, οπότε $(\alpha_1,\beta_1)=1$. Επειδή $\alpha^n\mid\beta^n$, θα πρέπει και $\alpha_1^n\mid\beta_1^n$. Άρα $\alpha_1^n\mid(\alpha_1^n,\beta_1^n)=(\alpha_1,\beta_1)^n=1$. Συνεπώς $\alpha_1=1$ και άρα $(\alpha,\beta)=\alpha$. Οπότε $\beta=\alpha\beta_1$ που σημαίνει ότι $\alpha\mid\beta$.

Μια άμεση εφαρμογή αυτού είναι η εξής: Αν ρ είναι ένας ρητός αριθμός και ο ρ^n, για κάποιο $n\in\mathbb{N}$, είναι ακέραιος αριθμός, τότε ο ρ είναι ακέραιος.

5. Δείχνουμε ότι, για κάθε $n\in\mathbb{N}$, $\alpha,\beta\in\mathbb{Z}$ με $\alpha^2+\beta^2\neq 0$ ισχύει

$$\left(\frac{\alpha^n-\beta^n}{\alpha-\beta},\alpha-\beta\right)=(n(\alpha,\beta)^{n-1},\alpha-\beta),$$

οπότε, αν $(\alpha,\beta)=1$, ισχύει

$$\left(\frac{\alpha^n-\beta^n}{\alpha-\beta},\alpha-\beta\right)=(n,\alpha-\beta).$$

Ισχύει $\dfrac{\alpha^n-\beta^n}{\alpha-\beta}=\alpha^{n-1}+\alpha^{n-2}\beta+\cdots+\alpha\beta^{n-2}+\beta^{n-1}$.

Προσθέτουμε και αφαιρούμε απ' το δεξί μέλος το $(n-1)\beta^{n-1}$ και έχουμε

$$\begin{aligned}\frac{\alpha^n-\beta^n}{\alpha-\beta}&=(\alpha^{n-1}-\beta^{n-1})+(\alpha^{n-2}\beta-\beta^{n-1})\\&\quad+\cdots+(\alpha\beta^{n-2}-\beta^{n-1})+n\beta^{n-1}\\&=(\alpha-\beta)\sum_0^{n-2}\alpha^{n-2-i}\beta^i+(\alpha-\beta)\beta\sum_0^{n-2}\alpha^{n-3-i}\beta^i\\&\quad+\cdots+(\alpha-\beta)\beta^{n-2}+n\beta^{n-1}=(\alpha-\beta)k+n\beta^{n-1},\quad k\in\mathbb{Z}.\end{aligned}$$

Απ' την ιδιότητα iv) έχουμε

$$\left(\frac{\alpha^n-\beta^n}{\alpha-\beta},\alpha-\beta\right)=((\alpha-\beta)k+n\beta^{n-1},\alpha-\beta)=(n\beta^{n-1},\alpha-\beta).$$

Με τον ίδιο τρόπο παίρνουμε επίσης ότι

$$\left(\frac{\alpha^n-\beta^n}{\alpha-\beta},\alpha-\beta\right)=(n\alpha^{n-1},\beta-\alpha)=(n\alpha^{n-1},\alpha-\beta).$$

Έστω $\delta=\left(\dfrac{\alpha^n-\beta^n}{\alpha-\beta},\alpha-\beta\right)$ και $\delta'=(n(\alpha,\beta)^{n-1},\alpha-\beta)$. Απ' το προηγούμενο παράδειγμα 3) έχουμε ότι $\delta'=(n(\alpha^{n-1},\beta^{n-1}),\alpha-\beta)$. Άρα $\delta'\mid n\alpha^{n-1}$ και $\delta'\mid n\beta^{n-1}$. Οπότε $\delta'\mid\delta$. Αλλά $\delta\mid n\alpha^{n-1}$ και $\delta\mid n\beta^{n-1}$ οπότε $\delta\mid n(\alpha^{n-1},\beta^{n-1})$ και άρα $\delta\mid\delta'$. Συνεπώς $\delta=\delta'$.

Για παράδειγμα, ισχύει $\left(\dfrac{\alpha^n-1}{\alpha-1},\alpha-1\right)=(n,\alpha-1)$.

6. Να αποδειχθεί ότι μ.κ.δ.$(\alpha^m-1,\alpha^n+1)=1$, όπου α, m και n είναι θετικοί ακέραιοι με $\alpha>1$ και m περιττός.

Έστω γ ένας κοινός διαιρέτης των α^m-1 και α^n+1. Οπότε $\alpha^m-1=\gamma\lambda$ και $\alpha^n+1=\gamma k$. Άρα

$$\alpha^{mn}=(\gamma\lambda+1)^n=(\gamma k-1)^m.$$

Αλλά

$$(\gamma\lambda+1)^n=\gamma t+1\quad\text{και}\quad(\gamma k-1)^m=\gamma s-1,$$

αφού το m είναι περιττός. Άρα

$$\gamma(s-t)=2, \quad \text{οπότε} \quad \gamma=1 \text{ ή } 2.$$

Αν ο α είναι περιττός, τότε οι α^m-1 και α^n+1 είναι άρτιοι, οπότε ο μ.κ.δ.$(\alpha^m-1,\alpha^n+1)=2$. Αν ο α είναι άρτιος, τότε οι α^m-1 και α^n+1 είναι περιττοί, οπότε ο μ.κ.δ.$(\alpha^m-1,\alpha^n+1)=1$.

7. Να δειχθεί ότι, για κάθε θετικούς ακεραίους $\alpha,\beta,n\neq 1$, ισχύει

$$(n^\alpha-1,n^\beta-1)=n^{(\alpha,\beta)}-1.$$

Έστω $\alpha=(\alpha,\beta)\alpha_1$ και $\beta=(\alpha,\beta)\beta_1$. Τότε

$$n^\alpha-1=(n^{(\alpha,\beta)}-1)\sum_{i=0}^{\alpha_1-1} n^{(\alpha,\beta)i}, \quad \text{δηλαδή} \quad n^{(\alpha,\beta)}-1 \mid n^\alpha-1$$

και

$$n^\beta-1=(n^{(\alpha,\beta)}-1)\sum_{i=0}^{\beta_1-1} n^{(\alpha,\beta)i}, \quad \text{δηλαδή} \quad n^{(\alpha,\beta)}-1 \mid n^\beta-1$$

Συνεπώς $n^{(\alpha,\beta)}-1 \mid (n^\alpha-1,n^\beta-1)$. Απ' το 1.3.6 γνωρίζουμε ότι υπάρχουν $x,y\in\mathbb{Z}$, τέτοιοι ώστε

$$(\alpha,\beta)=\alpha x+\beta y.$$

Προφανώς ένας απ' τους x και y πρέπει να είναι $\neq 0$. Επίσης, αν ένας απ' τους δύο είναι θετικός, έστω $x>0$, τότε $y\leq 0$, διότι αν ήταν $y>0$, τότε θα είχαμε $(\alpha,\beta)=\alpha x+\beta y\geq \alpha+\beta$, ενώ έχουμε $(\alpha,\beta)<\alpha+\beta$ αφού $(\alpha,\beta)\leq\alpha$ και $(\alpha,\beta)\leq\beta$. Φυσικά οι x και y δεν μπορούν να είναι και οι δύο αρνητικοί, αφού ο $(\alpha,\beta)>0$. Υποθέτουμε λοιπόν ότι $x>0$ και $y\geq 0$. Τότε

$$(n^\alpha-1,n^\beta-1)\mid n^{\alpha x}-1=(n^\alpha-1)\sum_{0}^{x-1} n^{\alpha i}$$

και

$$(n^\beta-1,n^\beta-1)\mid n^{\alpha x}-1=(n^\beta-1)\sum_{i=0}^{-y-1} n^{\beta i}$$

Οπότε

$$(n^\alpha - 1, n^\beta - 1) \mid n^{\alpha x} - 1 - n^{(\alpha,\beta)}(n^{-\beta y} - 1) = n^{(\alpha,\beta)} - 1.$$

Μπορούμε, επίσης, να αποδείξουμε την προηγούμενη ισότητα εφαρμόζοντας την Ευκλείδεια διαίρεση: Έστω $\alpha \geq \beta$, τότε $\alpha = \beta\pi + \upsilon$, $0 \leq \upsilon < \beta$. Επειδή $(n^{\beta\pi} - 1)n^\upsilon = (n^\beta - 1)kn^\upsilon$, όπου $k = \sum_0^{\pi-1} n^{\beta i}$, λόγω της ιδότητας iv) έχουμε

$$(n^\alpha - 1, n^\beta - 1) = (n^\alpha - 1 - (n^{\beta\pi} - 1)n^\upsilon, n^\beta - 1) = (n^\upsilon - 1, n^\beta - 1).$$

Αν συνεχίσουμε την ίδια διαδικασία για τον $(n^\upsilon - 1, n^\beta - 1)$ κ.ο.κ., όπως θα δούμε αμέσως, μετά από τον αλγόριθμο του Ευκλείδη, η διαδικασία αυτή θα τερματίσει στον $(n^{(\alpha,\beta)} - 1, 0) = n^{(\alpha,\beta)} - 1$.

8. Μερικές φορές για να υπολογίσουμε το μ.κ.δ. δύο ακεραίων α και β ακολουθούμε την εξής διαδικασία. Όπως θα δούμε στην **1.5** μπορούμε να γράψουμε $\alpha = 2^k\alpha_1$ και $\beta = 2^s\beta_1$, $k, s \in \mathbb{N}$, όπου α_1 και β_1 είναι περιττοί. Έστω ότι $k < s$, τότε λόγω της ιδιότητας ii) έχουμε

$$(\alpha, \beta) = 2^k(\alpha_1, 2^{s-k}\beta_1)$$

και λόγω της ιδιότητας vi) έχουμε $(\alpha, \beta) = 2^k(\alpha_1, (\alpha_1, 2^{sk})\beta_1) = 2^k(\alpha_1, \beta_1)$, αφού $2 \nmid \alpha_1$. Οπότε έχουμε να υπολογίσουμε το μ.κ.δ. δύο περιττών αριθμών α_1 και β_1. Γι' αυτούς έχουμε λόγω της ιδιότητας iv)

$$\begin{aligned}(\alpha_1, \beta_1) = (\alpha_1 - \beta_1, \beta_1) &= \left(2\frac{\alpha_1 - \beta_1}{2}, \beta_1\right) \\ &= \left(\frac{\alpha_1 - \beta_1}{2}, (\beta_1, 2)\beta_1\right) \\ &= \left(\frac{\alpha_1 - \beta_1}{2}, \beta_1\right).\end{aligned}$$

Για παράδειγμα, έστω $\alpha = 3696$, $\beta = 364$. Είναι $3696 = 24 \cdot 231$ και $\beta = 2^2 \cdot 91$. Οπότε

$$\begin{aligned}(\alpha, \beta) &= 2^2\left(\frac{231 - 91}{2}, 91\right) = 2^2(70, 91) = 2^2(35, 91) \\ &= 2^2(56, 35) = 2^2(7, 35) = 2^2 \cdot 7 = 28.\end{aligned}$$

9. Αποδεικνύουμε το Πόρισμα 1.3.4, ως πόρισμα της ιδιότητας vi). Έστω $\alpha = (\alpha,\beta)\alpha_1$ και $\beta = (\alpha,\beta)\beta_1$. Έχουμε ότι $\frac{\alpha\beta}{(\alpha,\beta)} = \alpha\Big(\frac{\beta}{(\alpha,\beta)}\Big)$ και $\frac{\alpha\beta}{(\alpha,\beta)} = \beta\Big(\frac{\alpha}{(\alpha,\beta)}\Big)$, δηλαδή ο $\frac{\alpha\beta}{(\alpha,\beta)}$ είναι ένα κοινό πολλαπλάσιο των α και β. Έστω k ένα κοινό πολλαπλάσιο των α και β, $k = \alpha k_1$, $k = \beta k_2$, $k_1, k_2 \in \mathbb{Z}$. Τότε $\frac{k}{(\alpha,\beta)} = \frac{\alpha}{(\alpha,\beta)}k_1 = \frac{\beta}{(\alpha,\beta)}k_2$. Επειδή $\Big(\frac{\alpha}{(\alpha,\beta)}, \frac{\beta}{(\alpha,\beta)}\Big) = 1$, λόγω της vi), $\frac{\alpha\beta}{(\alpha,\beta)^2}\Big|\frac{k}{(\alpha,\beta)}$. Οπότε $\frac{\alpha\beta}{(\alpha,\beta)}\Big|k$. Άρα $\frac{\alpha\beta}{(\alpha,\beta)} = [\alpha,\beta]$.

1.4 Ευκλείδειος Αλγόριθμος

Έστω $\alpha, \beta \in \mathbb{Z}$ με $\alpha^2+\beta^2 \neq 0$. Από το Θεώρημα 1.3.6, γνωρίζουμε ότι υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $(\alpha,\beta) = \alpha x + \beta y$. Η απόδειξη αυτού του θεωρήματος δεν παρέχει έναν τρόπο υπολογισμού των x και y και κατ' επέκταση του μ.κ.δ.(α,β). Μια πρακτική μέθοδος άμεσου υπολογισμού του μ.κ.δ.(α,β) αλλά και της εύρεσης ενός ζευγαριού $x, y \in \mathbb{Z}$ έτσι ώστε $(\alpha,\beta) = \alpha x + \beta y$ έδωσε πριν 2400 χρόνια ο Ευκλείδης στο βιβλίο του "Τα Στοιχεία του Ευκλείδη". Η μέθοδος αυτή στηρίζεται στις δύο βασικές ιδιότητες 1.3.10 i) και iv) και ονομάζεται Ευκλείδειος Αλγόριθμος.

Ο Αλγόριθμος βασίζεται στα εξής δύο βήματα.

Από την 1.3.10 i) μπορούμε να υποθέσουμε ότι $\alpha > \beta > 0$. Από την Ευκλείδεια διαίρεση υπάρχουν μοναδικοί $\pi, \upsilon \in \mathbb{Z}$ με $0 \leq \upsilon < \beta$ έτσι ώστε $\alpha = \beta\pi + \upsilon$.

1ο βήμα: Αν $\upsilon = 0$, δηλαδή αν $\beta \mid \alpha$, τότε $(\alpha,\beta) = \beta$ (ιδιότητα 1.3.10 i)).

2ο βήμα: Αν $\upsilon \neq 0$, τότε $(\alpha,\beta) = (\beta,\upsilon)$ (ιδιότητα 1.3.10 ii)).

Στην περίπτωση που είναι $\upsilon \neq 0$ επαναλαμβάνουμε την ίδια διαδικασία: Εφαρμόζουμε την Ευκλείδεια διαίρεση για τους β και υ, έστω $\beta = \upsilon\pi_1 + \upsilon_1$, όπου $0 \leq \upsilon_1 < \upsilon$. Αν $\upsilon_1 = 0$, τότε $(\alpha,\beta) = (\beta,\upsilon) = \upsilon$, διαφορετικά $(\alpha,\beta) = (\beta,\upsilon) = (\upsilon,\upsilon_1)$.

Συνεχίζοντας αυτή τη διαδικασία διαδοχικών Ευκλειδείων διαιρέσεων

έχουμε

$$\begin{aligned}
\alpha &= \beta\pi + \upsilon \\
\beta &= \upsilon\pi_1 + \upsilon_1 \\
\upsilon &= \upsilon_1\pi_2 + \upsilon_2 \\
\upsilon_1 &= \upsilon_2\pi_3 + \upsilon_3 \\
&\vdots \\
\upsilon_{i-1} &= \upsilon_i\pi_{i+1} + \upsilon_{i+1}
\end{aligned}$$

όπου

$$\alpha > \beta > \upsilon > \upsilon_1 > \cdots > \upsilon_{i+1} > 0 \quad \text{και}$$

$$(\alpha, \beta) = (\beta, \upsilon) = (\upsilon, \upsilon_1) = \cdots = (\upsilon_i, \upsilon_{i+1}).$$

Αυτή η διαδικασία όμως πρέπει να τερματίζει μετά από ένα πεπερασμένο πλήθος βημάτων, καθώς η αυστηρά φθίνουσα ακολουθία $\alpha > \beta > \upsilon > \cdots > \upsilon_{i+1} > 0$ αποτελείται από φυσικούς αριθμούς και άρα θα υπάρχει κάποιο n τέτοιο ώστε $\upsilon_{n+1} = 0$, οπότε $(\alpha, \beta) = (\upsilon_n, \upsilon_{n+1}) = \upsilon_n$. Δηλαδή ο μέγιστος κοινός διαιρέτης των α και β είναι το τελευταίο μη μηδενικό υπόλοιπο που προκύπτει από τις διαδοχικές προηγούμενες Ευκλείδειες διαιρέσεις.

☞ **Παράδειγμα.** Έστω $\alpha = 356$ και $\beta = 156$. Οι Ευκλείδειες διαδοχικές διαιρέσεις δίνουν

$$\begin{aligned}
356 &= 156 \cdot 2 + 44 \\
156 &= 44 \cdot 3 + 24 \\
44 &= 24 \cdot 1 + 20 \\
24 &= 20 \cdot 1 + 4 \\
20 &= 4 \cdot 5.
\end{aligned}$$

Οπότε $(356,\ 156) = 4$.

Παρατήρηση. Χρησιμοποιώντας την προηγούμενη διαδικασία μπορούμε να δώσουμε μια άλλη απόδειξη του 1.3.6, ως εξής.

Στον προηγούμενο Ευκλείδειο Αλγόριθμο για τους α και β, τον φυσικό αριθμό $n+1$ (για τον οποίο θεωρήσαμε ότι $\upsilon_{n+1} = 0$) τον ονομάζουμε

μήκος του Ευκλείδειου Αλγόριθμου των α και β και τον συμβολίζουμε με $\ell(\alpha,\beta)$, για παράδειγμα $\ell(356,\,156)=5$ (δηλαδή ο $\ell(\alpha,\beta)-1$ είναι το πλήθος των διαιρέσεων που απαιτούνται για να βρούμε το μ.κ.δ.).

Εφαρμόζοντας επαγωγή στο μήκος αυτό, έχουμε:

Αν $\ell(\alpha,\beta)=1$, δηλαδή αν $\beta \mid \alpha$, τότε $(\alpha,\beta)=\alpha\cdot 0+\beta 1$. Υποθέτουμε ότι για όλους τους αριθμούς α και β με $\ell(\alpha,\beta)<n+1$ υπάρχουν $x,y\in\mathbb{Z}$ έτσι ώστε $(\alpha,\beta)=\alpha x+\beta y$. Έστω ότι $\ell(\alpha,\beta)=n+1$, τότε από την Ευκλείδεια διαίρεση $\alpha=\beta\pi+\upsilon$ έχουμε $\ell(\beta,\upsilon)=n$ και συνεπώς υπάρχουν $x,y\in\mathbb{Z}$ έτσι ώστε $(\alpha,\beta)=(\beta,\upsilon)=\beta x+\upsilon y$. Αλλά $\upsilon=\alpha-\beta\pi$, οπότε $(\alpha,\beta)=\beta(x-\pi y)+\alpha\cdot y$. Άρα υπάρχουν $x'=y\in\mathbb{Z}$ και $y'=x-\pi y\in\mathbb{Z}$, τέτοιοι ώστε $(\alpha,\beta)=\alpha x'+\beta y'$.

Για την εύρεση ενός x και ενός y που ικανοποιεί την $\alpha x+\beta y=(\alpha,\beta)$ μπορούμε πάλι να χρησιμοποιήσουμε τον Ευκλείδειο Αλγόριθμο ως εξής: Από τις διαδοχικές Ευκλείδειες διαιρέσεις γράφουμε τα υπόλοιπα ως

$$\begin{aligned}
\upsilon &= \alpha-\beta\pi\\
\upsilon_1 &= \beta-\upsilon\pi_1\\
\upsilon_2 &= \upsilon-\upsilon_1\pi_2\\
&\vdots\\
\upsilon_{n-2} &= \upsilon_{n-4}-\upsilon_{n-3}\pi_{n-2}\\
\upsilon_{n-1} &= \upsilon_{n-2}-\upsilon_{n-2}\pi_{n-1}\\
\upsilon_n &= \upsilon_{n-2}-\upsilon_{n-1}\pi_n.
\end{aligned}$$

Οπότε έχουμε

$$\begin{aligned}
\upsilon_n &= \upsilon_{n-2}-(\upsilon_{n-3}-\upsilon_{n-2}\pi_{n-1})\pi_n\\
&= \upsilon_{n-2}(1+\pi_{n-1}\pi_n)+\upsilon_{n-3}(-\pi_n).
\end{aligned}$$

Στη συνέχεια αντικαθιστούμε το υ_{n-2} απ' την προηγούμενη έκφρασή του και παίρνουμε

$$\begin{aligned}
\upsilon_n &= (\upsilon_{n-4}-\upsilon_{n-3}\pi_{n-2})(1+\pi_{n-1}\pi_n)+\upsilon_{n-3}(-\pi_n)\\
&= \upsilon_{n-3}(-\pi_{n-2}(1+\pi_{n-1}\pi_n)-\pi_n)+\upsilon_{n-4}(1+\pi_{n-1}\pi_n).
\end{aligned}$$

Συνεχίζοντας με τον ίδιο τρόπο φθάνουμε τελικά σε μια παράσταση της μορφής που θέλουμε, δηλαδή $(\alpha, \beta) = \upsilon_n = \alpha x + \beta y$. Αυτή η διαδικασία δίνει μια νέα (κατασκευαστική) απόδειξη του 1.3.6.

Για παράδειγμα, για $\alpha = 356$, $\beta = 156$, έχουμε

$$\begin{aligned} 44 &= 356 - 156 \cdot 2 \\ 24 &= 156 - 44 \cdot 3 \\ 20 &= 44 - 24 \cdot 1 \\ 4 &= 24 - 20 \cdot 1. \end{aligned}$$

Οπότε

$$\begin{aligned} 4 = 24 - 20 \cdot 1 &= 24 - (44 - 24 \cdot 1) = 24 \cdot 2 - 44 = (156 - 44 \cdot 3)2 - 44 \\ &= 156 \cdot 2 + 44(-7) = 156 \cdot 2 + (356 - 156 \cdot 2)(-7) \\ &= 356(-7) + 156 \cdot (16). \end{aligned}$$

Άρα οι $x = -7$ και $y = 16$ δίνοαυν μια από τις (άπειρες) παραστάσεις του $(356,\ 156)$ της μορφής $\alpha x + \beta y, x, y \in \mathbb{Z}$.

Σημείωση. Για την εύρεση των x και y υπάρχουν και άλλοι τρόποι που ελαχιστοποιούν τους χρονοβόρους υπολογισμούς που προκύπτουν από τις διαδοχικές αντικαταστάσεις των υπολοίπων (βλέπε Oystein Ore [12] και S. P. Glasby: Extented Euclid's algorithm via backward recurrence relations, Math. Magazine 1999, 72(3), 228-230). Επίσης, αξίζει να αναφερθεί εδώ ότι το πλήθος των διαιρέσεων στον Ευκλείδειο αλγόριθμο για δύο θετικούς ακεραίους αριθμολύς είναι μικρότερο πέντε φορές από το πλήθος των δεκαδικών ψηφίων του μικρότερου των δύο αριθμών. Αυτό είναι ένα θεώρημα του Gabriel Lamé (1890).

Εδώ δείχνουμε ότι, αν $\upsilon_n = (\alpha, \beta)$, τότε $n < 2\dfrac{\log \beta}{\log 2} + 2$. Πράγματι ισχύει

$$\upsilon_{i+1} < \frac{\upsilon_{i-i}}{2}, \quad \forall\, i = 1, 2, \ldots$$

διότι, αν $\upsilon_i \leq \dfrac{\upsilon_{i-1}}{2}$, τότε $\upsilon_{i+1} < \upsilon_i \leq \dfrac{\upsilon_{i-1}}{2}$. Αλλά και αν $\upsilon_i < \dfrac{\upsilon_{i-i}}{2}$, τότε έχουμε απ' τις διαδοχικές διαιρέσεις: $\upsilon_{i+1} = \upsilon_{i-1} - \upsilon_i \pi_{i+1} < \upsilon_{i-1} - \dfrac{\upsilon_{i-i}}{2} =$

$\frac{v_{i-1}}{2}$. Οπότε

$$\beta > 2v_1 > 2^2 v_3 > \cdots > 2^{\frac{n-1}{2}} v_n \quad \text{ή}$$
$$\beta > 2v_1 > 2^2 v_3 > \cdots > 2^{\frac{n-2}{2}} v_n$$

αν ο n είναι περιττός ή άρτιος αντίστοιχα. Συνεπώς πάντα ισχύει $\beta > 2^{\frac{n-2}{2}}$ ή $\log \beta > \dfrac{n-2}{2} \log 2$.

Παρατήρηση. Όλες οι προηγούμενες ιδιότητες στην Πρόταση 1.3.10 μπορούν να αποδειχθούν εφαρμόζοντας τον αλγόριθμο του Ευκλείδη. Για παράδειγμα, ας αποδείξουμε την 1.3.10 v), δηλαδή αν $(\alpha, \beta) = 1$ και $\beta \mid \alpha\gamma$ τότε $\beta \mid \gamma$. Καθώς $(\alpha, \beta) = 1$ θα έχουμε $v_n = 1$. Πολλαπλασιάζοντας όλες τις Ευκλείδειες διαιρέσεις επί γ, υποθέτοντας ότι $\beta \mid \alpha\gamma$, ο β θα διαιρεί όλους τους ακεραίους $v_i\gamma$ και άρα και τον $\gamma = v_n\gamma$.

1.4.1 Εφαρμογή. Συνεχή Κλάσματα. Μια σημαντική εφαρμογή του Ευκλείδειου αλγόριθμου είναι ο καθορισμός της παράστασης ενός πραγματικού αριθμού σε συνεχές κλάσμα.

1.4.2 Ορισμός. *Ένα* ***πεπερασμένο συνεχές κλάσμα*** *είναι μια έκφραση της μορφής*

$$r = \alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\alpha_3 + \ddots + \cfrac{1}{\alpha_n}}}}$$

όπου κάθε α_i, $i \geq 1$, είναι ένας μη μηδενικός πραγματικός αριθμός. Αυτή η έκφραση συμβολίζεται συνήθως ως $\langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle$. Αν όλα τα α_i είναι ακέραιοι με όλα τα α_i, $i \geq 1$ θετικούς ακέραιους, τότε το συνεχές κλάσμα ονομάζεται ***απλό πεπερασμένο συνεχές κλάσμα.***

Αν $\alpha_0, \alpha_1, \alpha_2, \ldots$, είναι μια άπειρη ακολουθία πραγματικών αριθμών με $\alpha_i \neq 0$, $i \geq 1$, για την οποία η ακολουθία των πεπερασμένων συνεχών κλασμάτων $\langle \alpha_0 \rangle, \langle \alpha_0, \alpha_1 \rangle, \ldots, \langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle, \ldots$ συγκλίνει τότε το όριο αυτής της ακολουθίας το ονομάζουμε άπειρο συνεχές κλάσμα και

το συμβολίζουμε ως $\lim_{n\to\infty}\langle\alpha_0,\alpha_1,\ldots,\alpha_n\rangle = \langle\alpha_0,\alpha_1,\alpha_2,\ldots,\alpha_n,\ldots\rangle$. *Αν όλα τα* α_i *είναι ακέραιοι και* $\alpha_i > 0$, $\forall\ i = 1,2,\ldots$, *τότε το όριο αυτό ονομάζεται* **απλό άπειρο συνεχές κλάσμα**.

1.4.3 Θεώρημα. *Κάθε απλό πεπερασμένο συνεχές κλάσμα είναι ένας ρητός αριθμός. Αντίστροφα, κάθε ρητός αριθμός μπορεί να παρασταθεί ως ένα απλό πεπερασμένο συνεχές κλάσμα.*

Απόδειξη. Έστω $r = \langle\alpha_0,\alpha_1,\alpha_2,\ldots,\alpha_n\rangle$ ένα απλό πεπερασμένο συνεχές κλάσμα. Επειδή το r περιλαμβάνει ένα πεπερασμένο πλήθος προσθέσεων, πολλαπλασιασμών και διαιρέσεων ακέραιων αριθμών, ο r είναι ένας ρητός αριθμός. (Αυτός ο ισχυρισμός μπορεί να δειχθεί και επαγωγικά παρατηρώντας ότι $r = \alpha_0 + \dfrac{1}{\langle\alpha_1,\alpha_2,\ldots,\alpha_n\rangle}$).

Αντίστροφα, έστω $r = \dfrac{\alpha}{\beta}$ ένας ρητός αριθμός. Μπορούμε να υποθέσουμε ότι $\beta > 0$. Απ' τον Ευκλείδειο αλγόριθμο έχουμε

$$\begin{aligned}
\alpha &= \beta\alpha_0 + r_1 \\
\beta &= r_1\alpha_1 + r_2 \\
r_1 &= r_2\alpha_2 + r_3 \qquad\qquad 0 \le r_i < r_{i-1} \\
r_2 &= r_3\alpha_3 + r_4 \\
&\vdots \\
r_{n-2} &= r_{n-1}\alpha_n + r_n \\
r_{n-1} &= r_n\alpha_{n+1} + 0.
\end{aligned}$$

Οπότε παίρνουμε

$$\begin{aligned}
\frac{\alpha}{\beta} &= \alpha_0 + \frac{r_1}{\beta} = \alpha_0 + \cfrac{1}{\cfrac{\beta}{r_1}} \\
\frac{\beta}{r_1} &= \alpha_1 + \frac{r_2}{r_1} = \alpha_1 + \cfrac{1}{\cfrac{r_1}{r_2}} \\
\frac{r_1}{r_2} &= \alpha_2 + \frac{r_3}{r_2} = \alpha_2 + \cfrac{1}{\cfrac{r_2}{r_3}} \\
&\vdots \\
\frac{r_{n_1}}{r_n} &= \alpha_n + 0.
\end{aligned}$$

Τώρα, αντικαθιστώντας βρίσκουμε ότι

$$\frac{\alpha}{\beta} = \alpha_0 + \frac{1}{\frac{\beta}{r_1}} = \alpha_0 + \frac{1}{\alpha_1 + \frac{1}{\frac{r_1}{r_2}}}$$

$$= \cdots = \alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\alpha_3 + \ddots \cfrac{1}{\alpha_{n-1} + \cfrac{1}{\alpha_n}}}}} = \langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle. \quad \square$$

Παρατήρηση. Αν $\alpha_n > 1$, θέτοντας $\alpha_n = \alpha_n - 1 + \frac{1}{1}$ έχουμε $\langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle = \langle \alpha_0, \alpha_1, \ldots, \alpha_{n-1}, \alpha_n - 1, 1 \rangle$. Αν $\alpha_n = 1$ τότε $\langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle = \langle \alpha_0, \alpha_1, \ldots, \alpha_{n-1} + 1 \rangle$. Επαγωγικά εύκολα αποδεικνύεται ότι αυτές οι δύο παραστάσεις είναι οι μοναδικές παραστάσεις ενός ρητού αριθμού σε συνεχή κλάσματα.

☞ **Παράδειγμα.**

$$\frac{21}{13} = 1 + \frac{8}{13} = 1 + \frac{1}{\frac{13}{8}} = 1 + \frac{1}{1 + \frac{5}{8}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{3}{5}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{2}{3}}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}}.$$

Άρα $\frac{21}{13} = \langle 1, 1, 1, 1, 1, 1 \rangle = \langle 1, 1, 1, 1, 2 \rangle$.

Το επόμενο ερώτημα αφορά τα απλά άπειρα συνεχή κλάσματα. Είναι φυσικό να εικάσουμε ότι, όπως τα πεπερασμένα απλά συνεχή κλάσματα

ορίζουν τους ρητούς αριθμούς, αυτά ορίζουν τους άρρητους αριθμούς. Για τη μελέτη τέτοιων συνεχών κλασμάτων το κύριο εργαλείο δίδεται απ' τον εξής ορισμό.

1.4.4 Ορισμός. *Έστω $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n$ πραγματικοί αριθμοί με $\alpha_i > 0$, $\forall\ i = 1, 2, \ldots, n$. Το συνεχές κλάσμα $C_i = \langle \alpha_0, \alpha_1, \ldots, \alpha_i \rangle$, $0 \leq i \leq n$, ονομάζεται ο i-οστός συγκλίνων (ή προσεγγίζων) του συνεχούς κλάσματος $\langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle$.*

Έτσι έχουμε

$$C_0 = \langle \alpha_0 \rangle = \frac{\alpha_0}{1}$$

$$C_1 = \langle \alpha_0, \alpha_1 \rangle = \alpha_0 + \frac{1}{\alpha_1} = \frac{\alpha_0\alpha_1 + 1}{\alpha_1}$$

$$C_2 = \langle \alpha_0, \alpha_1, \alpha_2 \rangle = \alpha_0 + \frac{1}{\alpha_1 + \dfrac{1}{\alpha_2}} = \alpha_0 + \frac{1}{\dfrac{\alpha_1\alpha_2 + 1}{\alpha_2}} = \alpha_0 + \frac{\alpha_2}{\alpha_1\alpha_2 + 1}$$

$$= \frac{\alpha_0\alpha_1\alpha_2 + \alpha_2 + \alpha_0}{\alpha_1\alpha_2 + 1} = \frac{\alpha_2(\alpha_0\alpha_1 + 1) + \alpha_0}{\alpha_2(\alpha_1) + 1}$$

$$C_3 = \frac{\alpha_3(\alpha_2(\alpha_0\alpha_1 + 1) + \alpha_0) + \alpha_0\alpha_1 + 1}{\alpha_3(\alpha_1\alpha_2 + 1) + \alpha_1}.$$

Για την απλοποίηση αυτών των εκφράσεων ορίζουμε επαγωγικά τις εξής δύο ακολουθίες αριθμών που εξαρτώνται απ' το συνεχές κλάσμα $\langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle$

$$\begin{array}{ll}
p_{-1} = 1 & q_{-1} = 0 \\
p_0 = \alpha_0 & q_0 = 1 \\
p_1 = \alpha_1 p_0 + p_{-1} = \alpha_1\alpha_0 + 1 & q_1 = \alpha_1 q_0 + q_{-1} = \alpha_1 \\
p_2 = \alpha_2 p_1 + p_0 & q_2 = \alpha_2 q_1 + q_0 \\
p_3 = \alpha_3 p_2 + p_1 & q_3 = \alpha_3 q_2 + q_1 \\
\vdots & \vdots \\
p_k = \alpha_k p_{k-1} + p_{k-2} & q_k = \alpha_k q_{k-1} + q_{k-2} \\
\vdots & \vdots \\
p_n = \alpha_n p_{n-1} + p_{n-2} & q_n = \alpha_n q_{n-1} + q_{n-2}.
\end{array}$$

Αντικαθιστώντας αυτές τις τιμές στα C_0, C_1, C_2 και C_3 έχουμε $C_i = \dfrac{p_i}{q_i}$, $i = 0, 1, 2, 3$. Τώρα δείχνουμε ότι αυτό ισχύει για κάθε i.

1.4.5 Πρόταση. *Αν C_i είναι ο i-οστός συγκλίνων του $\langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle$ τότε αυτός είναι ίσος με*

$$C_i = \frac{p_i}{q_i} = \frac{\alpha_i p_{i-1} + p_{i-2}}{\alpha_i q_{i-1} + q_{i-2}}, \quad \textit{για κάθε } \ i, \quad 0 \leq i \leq n.$$

Απόδειξη. Είδαμε ότι η πρόταση ισχύει για $i = 0, 1, 2$ και 3. Υποθέτουμε ότι ισχύει για $i = m$, όπου $3 \leq m < n$, δηλαδή έχουμε

$$C_m = \frac{\alpha_i p_{m-1} + p_{m-2}}{\alpha_i q_{m-1} + q_{m-2}}.$$

Αλλά

$$\begin{aligned}
C_{m+1} = \langle \alpha_0, \alpha_1, \ldots, \alpha_m, \alpha_{m+1} \rangle &= \left\langle \alpha_0, \alpha_1, \ldots, \alpha_{m-1}, \alpha_m + \frac{1}{\alpha_{m+1} + 1} \right\rangle \\
&= \left\langle \alpha_0, \alpha_1, \ldots, \alpha_{m-1}, \frac{\alpha_m \alpha_{m+1} + 1}{\alpha_{m+1}} \right\rangle \\
&= \frac{\left(\frac{\alpha_m \alpha_{m+1} + 1}{\alpha_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(\frac{\alpha_m \alpha_{m+1} + 1}{\alpha_{m+1}}\right) q_{m-1} + q_{m-2}} \\
&= \frac{\alpha_m \alpha_{m+1} p_{m-1} + p_{m-1} + \alpha_{m+1} p_{m-2}}{\alpha_m \alpha_{m+1} q_{m-1} + q_{m-1} + \alpha_{m+1} q_{m-2}} \\
&= \frac{\alpha_{m+1}(\alpha_m p_{m-1} + p_{m-2}) + p_{m-1}}{\alpha_{m+1}(\alpha_m q_{m-1} + q_{m-2}) + q_{m-1}} \\
&= \frac{\alpha_{m+1} p_m + p_{m-1}}{\alpha_{m+1} q_m + q_{m-1}} = \frac{p_{m+1}}{q_{m+1}}.
\end{aligned}$$

Οπότε η πρόταση ισχύει και για $m + 1$. □

1.4.6 Πόρισμα. *Έστω $C_i = \dfrac{p_i}{q_i}$ ο i-οστός συγκλίνων του $\langle \alpha_0, \alpha_1, \ldots, \alpha_k \rangle$. Τότε ισχύει*

$$p_i q_{i-1} - q_i p_{i-1} = (-1)^{i-1}$$

και πολλαπλασιάζοντας επί α_i παίρνουμε

$$p_i q_{i-2} - q_i p_{i-2} = (-1)^i \alpha_i.$$

Απόδειξη. Εφαρμόζουμε επαγωγή. Για $i = 1$ έχουμε

$$p_1 q_0 - q_1 p_0 = (\alpha_1 \alpha_0 + 1) \cdot 1 - \alpha_1 \cdot \alpha_0 = 1 = (-1)^{1-1}.$$

Υποθέτουμε ότι η ισότητα είναι αληθής για τα $C_1, C_2, \ldots, C_{i-1}$. Απ' την προηγούμενη πρόταση έχουμε

$$\begin{aligned} p_i q_{i-1} - q_i p_{i-1} &= (\alpha_i p_{i-1} + p_{i-2}) q_{i-1} - (\alpha_i q_{i-1} + q_{i-2}) p_{i-1} \\ &= p_{i-2} q_{i-1} - q_{i-2} p_{i-1} = -(p_{i-1} q_{i-2} - q_{i-1} p_{i-2}) \\ &= (-1)^{i-1} \text{ (απ' την επαγωγική υπόθεση).} \end{aligned}$$

□

1.4.7 Πόρισμα. *Υποθέτουμε ότι το $\langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle$ είναι απλό. Τότε οι ακέραιοι p_i και q_i, $i \geq 0$ είναι σχετικά πρώτοι μεταξύ τους. Το ίδιο ισχύει και για τα ζευγάρια των ακεραίων p_i, p_{i+1} και q_i, q_{i+1}.*

Απόδειξη. Απ' το προηγούμενο πόρισμα έχουμε

$$p_i (-1)^i q_{i-1} + q_i (-1)^{i+1} p_{i-1} = 1.$$

Όμοια αποδεικνύεται και για τους άλλους ακέραιους. □

1.4.8 Πόρισμα. *Αν $C_i = \dfrac{p_i}{q_i}$ είναι ο i-οστός συγκλίνων του απλού συνεχούς κλάσματος $\langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle$, τότε για κάθε i ισχύει*

$$C_i - C_{i-1} = \frac{(-1)^{i-1}}{q_i q_{i-1}}, \quad \textit{για} \quad 1 \leq i \leq n$$

και

$$C_i - C_{i-2} = \frac{\alpha_i (-1)^i}{q_i q_{i-2}}, \quad \textit{για} \quad 2 \leq i \leq n.$$

Απόδειξη. Διαιρούμε τις σχέσεις στο προηγούμενο Πόρισμα 1.4.6 δια $q_i q_{i-1}$. □

Το επόμενο λήμμα είναι το κύριο εργαλείο για τη μελέτη των άπειρων απλών συνεχών κλασμάτων.

1.4.9 Λήμμα. *Έστω $C_i = \dfrac{p_i}{q_i}$ ο i-οστός συγκλίνων του απλού συνεχούς κλάσματος $a = \langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle$. Τότε ισχύει η διάταξη*

$$C_1 > C_3 > C_5 > \cdots$$

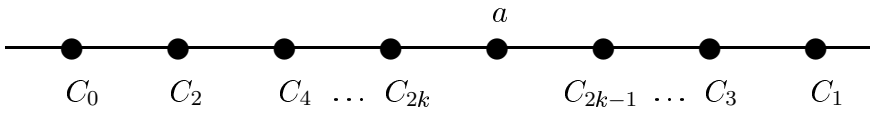
$$C_0 < C_2 < C_4 < \cdots$$

Δηλαδή η ακολουθία C_i των i-οστών συγκλινόντων με i περιττό (αντίστοιχα με i άρτιο) είναι φθίνουσα (αντίστοιχα αύξουσα). Επίσης ισχύει

$$C_{2k+1} > C_{2k}, \quad k = 0, 1, 2, \ldots \quad \textit{και συνεπώς}$$

$$C_{2j-1} > C_{2s+2j-1} > C_{2s+2j} > C_{2s}$$

δηλαδή, κάθε συγκλίνων με περιττό δείκτη είναι μεγαλύτερος από κάθε συγκλίνοντα με άρτιο δείκτη



Απόδειξη. Απ' το Πόρισμα 1.4.7, για $i = 2, 3, \ldots$ έχουμε

$$C_i - C_{i-2} = \frac{\alpha_i(-1)^i}{q_i q_{i-2}}$$

οπότε, αν i είναι άρτιος, πρέπει $C_i > C_{i-2}$ και αν i είναι περιττός, πρέπει $C_i < C_{i-2}$. Επίσης έχουμε

$$C_{2j} - C_{2j-1} = \frac{(-1)^{2j-1}}{q_{2j} q_{2j-1}} < 0.$$

δηλαδή $C_{2j} < C_{2j-1}$. □

1.4.10 Λήμμα. *Έστω $\alpha_0, \alpha_1, \ldots, \alpha_i, \ldots$ μια ακολουθία ακεραίων με $\alpha_i > 0$ για $i \geq 1$. Έστω $C_i = \langle \alpha_0, \alpha_1, \ldots, \alpha_i \rangle$. Τότε υπάρχει το $\lim_{i\to\infty} C_i$ και είναι πεπερασμένο, δηλαδή ορίζεται το απλό άπειρο συνεχές κλάσμα $\langle \alpha_0, \alpha_1, \ldots \rangle$.*

Απόδειξη. Μπορούμε να θεωρήσουμε κάθε C_i ως έναν απ' τους συγκλίνοντες ενός απλού πεπερασμένου συνεχούς κλάσματος. Απ' το προηγούμενο λήμμα έχουμε

$$C_2 < C_4 < C_6 < \cdots < C_5 < C_3 < C_1.$$

Η ακολουθία C_{2j+1} είναι μια περατομένη φθίνουσα ακολουθία πραγματικών αριθμών και συνεπώς έχει ένα πεπερασμένο όριο α. Καθώς κάθε C_{2j+1}

είναι μεγαλύτερος από κάθε C_{2s}, ο α είναι μεγαλύτερος ή ίσος από κάθε C_{2s}. Αλλά $\lim\limits_{i\to\infty} q_i = \infty$ αφού $q_i - q_{i-1} = (\alpha_i - 1)q_{i-1} + q_{i-2} > q_{i-2} > 1$, για $i > 1$, οπότε $q_{i-1} < q_i$, $\forall\, i$, διλαδή η ακολουθία q_i είναι μια αύξουσα ακολουθία ακεραίων.

Συνεπώς έχουμε

$$\begin{aligned} 0 &\le \lim_{i\to\infty}(\alpha - C_{2i}) \le \lim_{i\to\infty}(C_{2i+1} - C_{2i}) \\ &= \lim_{i\to\infty} \frac{(-1)^{2i+1-1}}{q_{2i+1}q_{2i}} = 0. \end{aligned}$$

Άρα

$$\lim_{i\to\infty} C_{2i} = \lim_{i\to\infty} C_{2i+1} = \alpha. \ \square$$

1.4.11 Θεώρημα. *Έστω $\alpha_0, \alpha_1, \ldots, \alpha_i, \ldots$ ακέραιοι με $\alpha_i \ge 1$, $\forall\, i = 1, 2, \ldots$. Τότε το απλό άπειρο συνεχές κλάσμα $\alpha = \langle \alpha_0, \alpha_1, \ldots \rangle$ είναι ένας άρρητος αριθμός.*

Απόδειξη. Απ' τα προηγούμενα έχουμε

$$C_{2i} < \alpha < C_{2i+1}, \quad i = 1, 2, \ldots$$

οπότε $0 < \alpha - C_{2i} < C_{2i+1} - C_{2i}$.

Αλλά $C_{2i+1} - C_{2i} = \dfrac{1}{q_{2i+1}q_{2i}}$. Οπότε

$$0 < \alpha - C_{2i} = \alpha - \frac{p_{2i}}{q_{2i}} < \frac{1}{q_{2i+1}q_{2i}}$$

και συνεπώς έχουμε

$$0 < \alpha q_{2i} - p_{2i} < \frac{1}{q_{2i+1}}.$$

Αν ο α ήταν ρητός, έστω $\alpha = \dfrac{m}{n}$, $m, n \in \mathbb{Z}$, $n \neq 0$, τότε θα είχαμε

$$0 < \frac{mq_{2i}}{n} - p_{2i} < \frac{1}{q_{2i+1}}$$

ή ισοδύναμα

$$0 < mq_{2i} - np_{2i} < \frac{n}{q_{2i+1}}.$$

Επειδή η ακολουθία q_j είναι αύξουσα ακολουθία ακεραίων, μπορούμε να επιλέξουμε ένα i αρκετά μεγάλο, έτσι ώστε $\beta < q_{2i+1}$, οπότε θα είχαμε

$$0 < mq_{2i} - np_{2i} < 1$$

που είναι άτοπο, αφού ο $mq_{2i} - np_{2i}$ είναι ακέραιος.

Συνεπώς το απλό άπειρο συνεχές κλάσμα α είναι ένας άρρητος αριθμός. □

Ισχύει και το αντίστροφο.

1.4.12 Θεώρημα. *Κάθε άρρητος αριθμός μπορεί να παρασταθεί ως ένα απλό άπειρο συνεχές κλάσμα. Επιπλέον, μια τέτοια παράσταση είναι μοναδική.*

Απόδειξη. Έστω x ένας άρρητος αριθμός. Επαγωγικά ορίζουμε

$$x_0 = x, \quad x_{k+1} = \frac{1}{x_k - \alpha_k}, \quad k = 0, 1, 2, \ldots$$

όπου με $\alpha_k = [x_k]$ συμβολίζουμε το ακέραιο μέρος του x_k. Θα δείξουμε ότι $x = \langle \alpha_0, \alpha_1, \alpha_2, \ldots \rangle$. Κατ' αρχάς, επειδή ο x είναι άρρητος, επαγωγικά ο x_k είναι επίσης άρρητος (διότι διαφορετικά απ' την $x_k = \dfrac{1}{x_{k-1} - [x_{k-1}]}$ θα προέκυπτε ότι ο $x_{k-1} = \dfrac{1}{x_k} + [x_{k-1}]$ θα ήταν ρητός που δεν ισχύει σύμφωνα με την επαγωγική υπόθεση). Συνεπώς $x_k \neq [x_k]$ και άρα $[x]_k < x_k < [x_k] + 1$, οπότε $0 < x_k - [x_k] < 1$. Άρα

$$x_{k+1} = \frac{1}{x_k - [x_k]} > 1$$

και συνεπώς $[x_{k+1}] \geq 1$, για κάθε $k = 0, 1, \ldots$.

Τώρα έχουμε

$$\begin{aligned} x = x_0 &= [x_0] + \frac{1}{x_1} = \langle [x_0], x_1 \rangle \\ &= [x_0] + \cfrac{1}{[x_2] + \dfrac{1}{x_2}} = \langle [x_0], [x_1], x_2 \rangle \\ &= \cdots \\ &\vdots \\ &= \langle [x_0], [x_1], \ldots, [x_k], x_{k+1} \rangle. \end{aligned}$$

Απ' την Πρόταση 1.4.5 έχουμε

$$x = \frac{x_{k+1}p_k + p_{k-1}}{x_{k+1}q_k + q_{k-1}}, \quad \text{οπότε}$$

$$x - C_k = \frac{x_{k+1}p_k + p_{k-1}}{x_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{(x_{k+1}q_k + q_{k-1})q_k}$$

λόγω του Πορίσματος 1.4.6. Τώρα, επειδή $x_{k+1} > [x_{k+1}]$ έχουμε

$$|x - C_k| = \frac{1}{(x_{k+1}q_k + q_{k-1})q_k} < \frac{1}{([x_{k+1}]q_k + q_{k-1})q_k} = \frac{1}{q_{k+1}q_k}$$

και καθώς οι ακέραιοι q_k αποτελούν αύξουσα ακολουθία προκύπτει ότι

$$x = \lim C_k = \langle [x_0], [x_1], [x_2], \ldots \rangle.$$

Απομένει να δείξουμε τη μοναδικότητα. Έστω ότι ο άρρητος αριθμός x έχει δύο παραστάσεις

$$\langle \alpha_0, \alpha_1, \ldots \rangle \quad \text{και} \quad \langle \beta_0, \beta_1, \beta_2, \ldots \rangle.$$

Έχουμε ότι $C_0 = \alpha_0$ και $C_1 = \alpha_0 + \dfrac{1}{\alpha_1}$. Επίσης γνωρίζουμε ότι $C_0 < x < C_1$, δηλαδή $\alpha_0 < x < \alpha_0 + \dfrac{1}{\alpha_1}$ οπότε $\alpha_0 < x < \alpha_0 + 1$ και άρα $\alpha_0 = [x]$. Επίσης $\beta_0 = [x]$, δηλαδή $\alpha_0 = \beta_0$ και έχουμε

$$x = \lim_{k\to\infty} C_k = \lim \left(\alpha_0 + \frac{1}{\langle \alpha_1, \alpha_2, -\alpha_k \rangle} \right) = \alpha_0 + \frac{1}{\lim\limits_{k\to\infty} \langle \alpha_1, \alpha_2, \ldots, \alpha_k \rangle}$$

$$= \alpha_0 + \frac{1}{\langle \alpha_1, \alpha_2, \ldots, \alpha_i, \ldots \rangle}. \quad \text{Συνεπώς}$$

$$x = \alpha_0 + \frac{1}{\langle \alpha_1, \alpha_2, \ldots, \rangle} = \beta_0 + \frac{1}{\langle \beta_1, \beta_2, \ldots, \rangle}.$$

Επειδή $\alpha_0 = \beta_0 = [x]$ προκύπτει ότι

$$\langle \alpha_1, \alpha_2, \ldots, \rangle = \langle \beta_1, \beta_2, \ldots, \rangle$$

απ' το οποίο προκύπτει ότι $\alpha_1 = \beta_1$. Έτσι επαγωγικά έχουμε $\beta_k = \alpha_k$, $\forall\, k = 0, 1, 2, \ldots$.

Τελικό Συμπέρασμα: Υπάρχει $1-1$ αντιστοιχία μεταξύ των άρρητων αριθμών και των απλών άπειρων συνεχών κλασμάτων. Υπάρχει $1-1$ αντιστοιχία μεταξύ των ρητών αριθμών και των απλών πεπερασμένων συνεχών κλασμάτων της μορφής $\langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle$ με $\alpha_n > 1$.

Αν x είναι ένας άρρητος και p_n/q_n είναι ο n-ιοστός συγκλίνων, τότε $\left| x - \dfrac{p_n}{q_n} \right| < \dfrac{1}{q_2}$. Μπορεί να δειχθεί ότι οι συγκλίνοντες $\dfrac{p_n}{q_n}$ είναι οι καλύτερες προσεγγίσεις του x με την έννοια ότι η τιμή τους είναι πιο κοντά στο x από κάθε άλλο ρητό $\dfrac{\alpha}{\beta}$ όπου $1 \leq \beta \leq q_n$.

☞ **Παραδείγματα.** $\sqrt{2}$. Καθώς $[\sqrt{2}] = 1$, έχουμε $\sqrt{2} = 1 + (\sqrt{2} - 1)$ οπότε $\sqrt{2} = 1 + \dfrac{1}{\dfrac{1}{\sqrt{2}-1}}$. Αλλά $\dfrac{1}{\sqrt{2}-1} = \sqrt{2}+1$ και συνεπώς $\sqrt{2} = 1 + \dfrac{1}{\sqrt{2}+1}$. Αλλά $\sqrt{2}+1 = 2 + (\sqrt{2}+1-2) = 2 + (\sqrt{2}-1) = 2 + \dfrac{1}{\sqrt{2}+1}$. Έτσι έχουμε $\sqrt{2} = \langle 1, 2, \sqrt{2}+1 \rangle = \langle 1, 2, 2, 2, \ldots \rangle$.

$\sqrt{3}$. Καθώς $[\sqrt{3}] = 1$, έχουμε $\sqrt{3} = 1 + (\sqrt{3}-1) = 1 + \dfrac{1}{\dfrac{1}{\sqrt{3}-1}}$. Αλλά

$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} = \frac{2+(\sqrt{3}-1)}{2} = 1 + \frac{1}{\dfrac{2}{\sqrt{3}-1}} \quad \text{και}$$

$$\frac{1}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{3-1} = \sqrt{3}+1 = 2 + (\sqrt{3}-1) = 2 + \frac{1}{\dfrac{1}{\sqrt{3}-1}}.$$

Οπότε

$$\frac{1}{\sqrt{3}-1} = \left\langle 1, \frac{2}{\sqrt{3}-1} \right\rangle = \left\langle 1, 2, \frac{1}{\sqrt{3}-1} \right\rangle = \left\langle 1, 2, 1, \frac{1}{\sqrt{3}-1} \right\rangle.$$

Άρα

$$\sqrt{3} = \left\langle 1, \frac{1}{\sqrt{3}-1} \right\rangle = \langle 1, 1, 2, 1, 2, 1, 2, \ldots \rangle.$$

Θα εφαρμόσουμε τα συνεχή κλάσματα πιο κάτω στις Διοφαντικές εξισώσεις.

1.5 Πρώτοι Αριθμοί – Θεμελιώδες Θεώρημα της Αριθμητικής

1.5.1 Ορισμός. *Ένας φυσικός αριθμός > 1 θα καλείται* ***πρώτος αριθμός*** *ή απλά πρώτος, αν οι μόνοι διαιρέτες του είναι οι ± 1 και $\pm p$. Ένας φυσικός αριθμός $n > 1$ που δεν είναι πρώτος θα καλείται* ***σύνθετος αριθμός****.*

Συνεπώς ένας θετικός ακέραιος $p > 1$ είναι πρώτος, αν και μόνον αν για κάθε $n \in \mathbb{Z}$ ισχύει $(p, n) = 1$ ή $(p, n) = p$, δηλαδή ή ο p είναι σχετικά πρώτος προς τον n ή ο p διαιρεί τον n.

Επειδή, κάθε άρτιος αριθμός διαιρείται δια του 2, από τον ορισμό προκύπτει ότι όλοι οι πρώτοι εκτός από τον 2 είναι περιττοί αριθμοί. Επειδή ένας από οποιουσδήποτε δύο διαδοχικούς ακεραίους ο ένας είναι άρτιος και ο άλλος περιττός, οι μόνοι διαδοχικοί πρώτοι είναι οι 2 και 3.

Οι πρώτοι που είναι μικρότεροι του 100 είναι οι εξής 25 αριθμοί: 2, 3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83 και 97. Στο τέλος του βιβλίου παραθέτουμε σε κατάλογο τους 10.000 πρώτους που είναι μεταξύ του 1 και 104.729.

Σημειώνουμε ότι στον Ορισμό 1.5.1, ο αριθμός 1 κατά συνθήκη δεν θεωρείται ούτε πρώτος ούτε σύνθετος αριθμός. Αποδεχόμαστε αυτή τη συνθήκη διότι αφ' ενός οι διατυπώσεις πολλών θεωρημάτων και αποτελεσμάτων που θα δούμε πιο κάτω γίνονται απλούστερες και αφ' ετέρου οι ιδιότητες του 1 είναι διαφορετικές απ' αυτές των πρώτων και των σύνθετων αριθμών.

1.5.2 Λήμμα. *Κάθε φυσικός > 1 είναι ή ένας πρώτος αριθμός ή το γινόμενο πρώτων αριθμών.*

Απόδειξη. Έστω $n \in \mathbb{N}$, $n > 1$. Υποθέτουμε ότι κάθε φυσικός m, $1 < m < n$, είτε είναι πρώτος ή είναι γινόμενο πρώτων. Αν ο n δεν είναι πρώτος, τότε έχει έναν διαιρέτη α, $1 < \alpha < n$ και $n = \alpha\beta$ για κάποιον $\beta \in \mathbb{N}$ με $1 < \beta < n$ (γιατί;). Οπότε οι α και β είναι είτε πρώτοι ή γινόμενο πρώτων. Άρα ο n αν δεν είναι πρώτος, αυτός είναι γι-

νόμενο πρώτων. Συνεπώς επαγωγικά το ζητούμενο ισχύει για κάθε $n \in \mathbb{N}$, $n > 1$. □

Το Λήμμα 1.5.2 μας λέει ότι οι πρώτοι αριθμοί είναι πολλαπλασιαστικά οι "θεμέλιοι λίθοι" για την κατασκευή των φυσικών αριθμών. Έτσι είναι φυσικό ένα μεγάλο μέρος της Θεωρίας Αριθμών να επικεντρώνεται στη μελέτη των πρώτων αριθμών.

Από τον ορισμό των πρώτων και από το 1.3.10 v) προκύπτει άμεσα το εξής:

1.5.3 Λήμμα. *(**Ευκλείδης**). Αν p είναι ένας πρώτος αριθμός που διαιρεί το γινόμενο $\alpha\beta$, $\alpha, \beta \in \mathbb{Z}$, τότε ο p διαιρεί τουλάχιστον έναν απ' τους α και β.*

Σημειώνουμε ότι ισχύει και το αντίστροφο, δηλαδή αν $p > 1$ είναι ένας φυσικός αριθμός που για οποιουσδήποτε ακεραίους α και β ο p διαιρεί τουλάχιστον έναν απ' τους δύο, όταν ο p διαιρεί το γινόμενό τους $\alpha\beta$, τότε ο p είναι πρώτος. Πράγματι, αν υποθέσουμε ότι ο p ήταν σύνθετος, τότε $p = \alpha\beta$ με $1 < \alpha < p$ και $1 < \beta < p$ και έτσι θα υπήρχαν δύο ακέραιοι οι α και β που και οι δύο δεν θα διαιρούντο δια του p αλλά ο p διαιρεί τον $\alpha\beta$.

1.5.4 Πόρισμα. *Αν p είναι πρώτος και $p \mid \alpha_1\alpha_2\cdots\alpha_n$, $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$, τότε $p \mid \alpha_i$, για κάποιο $i = 1, 2, \ldots, n$. Ειδικότερα, αν οι $\alpha_1, \alpha_2 \ldots, \alpha_n$ είναι πρώτοι, τότε $p = \alpha_i$, για κάποιο i.*

Απόδειξη. Εφαρμόζουμε επαγωγή στο n χρησιμοποιώντας το προηγούμενο λήμμα. □

Από το 1.5.4 άμεσα προκύπτει.

1.5.5 Πόρισμα. *Αν p είναι πρώτος και $p \mid \alpha^k$, $\alpha \in \mathbb{Z}$, τότε $p^k \mid \alpha^k$.*

Τώρα θα λέμε ότι **ένας φυσικός αριθμός > 1 αναλύεται μοναδικά σε γινόμενο πρώτων παραγόντων** αν για δοσμένους πρώτους $p_1, p_2, \ldots, p_r$ και $q_1, q_2, \ldots, q_s$ τέτοιους ώστε

$$n = p_1p_2\cdots p_r = q_1q_2\cdots q_s$$

όσες φορές εμφανίζεται ένας πρώτος μεταξύ των $p_1, p_2, \ldots, p_r$ τόσες φορές εμφανίζεται αυτός μεταξύ των $q_1, q_2, \ldots, q_s$. (Σημειώνουμε ότι απ' αυτό προκύπτει $r = s$).

Με αυτή την ορολογία αποδεικνύουμε τώρα το **Θεμελιώδες Θεώρημα της Αριθμητικής** (μερικές φορές αυτό αναφέρεται και ως **Θεώρημα Μοναδικής Παραγοντοποίησης**).

1.5.6 Θεώρημα. *Κάθε φυσικός αριθμός $n > 1$ αναλύεται μονάδικά σε γινόμενο πρώτων παραγόντων.*

1η Απόδειξη. Σ' αυτή την απόδειξη χρησιμοποιούμε το 1.5.4. Μπορούμε να υποθέσουμε ότι ο n είναι σύνθετος αριθμός. Υποθέτουμε ότι κάθε σύνθετος αριθμός μικρότερος του n αναλύεται μοναδικά σε πρώτους παράγοντες. Δείχνουμε ότι τότε και ο n αναλύεται μοναδικά σε πρώτους παράγοντες, οπότε το αποτέλεσμα έπεται από την Αρχή της Πλήρους Μαθηματικής Επαγωγής στο n.

Έστω λοιπόν ότι

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

όπου $p_1, p_2, \ldots, p_r$ και $q_1, q_2, \ldots, q_s$ είναι πρώτοι και $p_1 \leq p_2 \leq \cdots \leq p_r$, $q_1 \leq q_2 \leq \cdots \leq q_s$. Πρέπει να δείξουμε ότι $r = s$ και $p_i = q_i$ για κάθε $i = 1, 2, \ldots, r$.

Έστω p ο μικρότερος πρώτος που διαιρεί τον n. Τότε, λόγω του 1.5.4, $p = p_i$, για κάποιο $i = 1, 2, \ldots, r$, και επειδή $p \leq p_1$ θα πρέπει $p = p_1$. Όμοια $p = q_1$, οπότε $p_1 = q_1$. Έστω $m = \dfrac{n}{p}$. Τότε

$$m = p_2 p_3 \cdots p_r = q_2 \cdots q_s.$$

Αλλά τότε $r = s$ και $p_i = q_i$, $i = 1, \ldots, r$, αφού $m < n$. Άρα ο n αναλύεται μοναδικά σε πρώτους παράγοντες. Έτσι έχουμε δείξει ότι, αν όλοι οι σύνθετοι αριθμοί m, $1 < m < n$ αναλύονται μοναδικά σε πρώτους παράγοντες, το ίδιο ισχύει και για όλους τους σύνθετους αριθμούς m $1 < m < n + 1$.

Άρα όλοι οι σύνθετοι αριθμοί αναλύονται μοναδικά σε πρώτους παράγοντες.

2η Απόδειξη. Σ' αυτή την απόδειξη εφαρμόζουμε άμεσα την αρχή του

ελαχίστου και είναι ανεξάρτητη του Λήμματος του Ευκλείδη, δηλαδή του 1.5.4.

Ισχυριζόμαστε ότι η ανάλυση ενός φυσικού αριθμού $n > 1$ είναι μοναδική. Ας υποθέσουμε ότι ο ισχυρισμός αυτός δεν ισχύει. Δηλαδή υποθέτουμε ότι το σύνολο των φυσικών αριθμών $n > 1$ που έχουν δύο διαφορετικές αναλύσεις σε γινόμενο πρώτων δεν είναι κενό. Τότε απ' την αρχή του ελαχίστου αυτό το σύνολο έχει ένα ελάχιστο στοιχείο, έστω n, όπου

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

με $p_1 \leq p_2 \leq \cdots \leq p_r$, $q_1 \leq q_2 \leq \cdots q_s$.

Κάθε p_i είναι διάφορος από κάθε q_i, διότι διαφορετικά αν υπήρχε κοινός πρώτος παράγοντας θα παίρναμε κάποιον $n' < n$ με την ίδια ιδιότητα που έχει ο n (που δεν μπορεί να ισχύει λόγω της υπόθεσης ότι ο n είναι ο μικρότερος μ' αυτή την ιδιότητα). Έστω ότι $p_1 < q_1$. Θεωρούμε το σύνθετο αριθμό

$$m = p_1 q_2 q_3 \cdots q_s.$$

Ο φυσικός αριθμός $\ell = n - m = (q_1 - p_1) q_2 \cdots q_s$ που είναι μικρότερος από τον n διαιρείται δια του p_1, αφού $p_1 \mid n$ και $p_1 \mid m$. Οπότε ο ℓ αναλύεται μοναδικά σε πρώτους παράγοντες ένας εκ των οποίων είναι ο p_1. Έστω

$$\ell = p_1 t_2 t_2 \cdots t_k$$

η ανάλυση του ℓ σε πρώτους παράγοντες. Αν ήταν ο αριθμός $q_1 - p_1 = 1$, τότε ο ℓ θα είχε δύο αναλύσεις σε πρώτους παράγοντες, η μια θα περιείχε τον p_1 και η άλλη δεν θα τον περιείχε, οπότε, επειδή $\ell < n$, πρέπει $q_1 - p_1 \neq 1$. Συνεπώς μπορούμε να γράψουμε τον $q_1 - p_1$ ως γινόμενο πρώτων αριθμών, έστω

$$q_1 - p_1 = h_1 h_2 \cdots h_t.$$

Έτσι έχουμε $\ell = h_1 h_2 \cdots h_t q_2 \cdots q_s$. Αυτή είναι μια ανάλυση του ℓ σε πρώτους που δεν περιέχει τον p_1, αφού $p_1 \nmid q_1 - p_1$ και $p_1 \neq q_i$, $i = 1, 2, \ldots, s$. Όπως όμως είδαμε ο ℓ έχει και άλλη ανάλυση σε πρώτους που περιέχει τον p_1. Επειδή $\ell < n$, αυτό είναι άτοπο, αφού ο n είναι ο μικρότερος αριθμός με περισσότερες της μιας αναλύσεις σε πρώτους παράγοντες. Άρα δεν

υπάρχει κανένας φυσικός σύνθετος αριθμός με περισσότερες της μιας αναλύσεις σε πρώτους παράγοντες. □

Σημείωση. Η πρώτη απόδειξη δόθηκε από τον Ευκλείδη ενώ η δεύτερη από τον Zermelo.

Παρατήρηση. **1.** Αν είχαμε συμπεριλάβει τον αριθμό 1 στους πρώτους αριθμούς, τότε θα έπρεπε να αναδιατυπώναμε το προηγούμενο θεώρημα επιτρέποντας διαφορετικές παραγοντοποιήσεις, για παράδειγμα $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3$.

2. Υποθέτοντας ότι ισχύει το Λήμμα 1.5.2, τότε το Λήμμα του Ευκλείδη και το Θεμελιώδες Θεώρημα της Αριθμητικής είναι ισοδύναμα. Πράγματι, η μία κατεύθυνση είναι ακριβώς το Θεώρημα 1.5.6. Υποθέτουμε ότι ισχύει το Θεώρημα 1.5.6 και έστω ότι p είναι ένας πρώτος που διαιρεί το γινόμενο $\alpha\beta$ δύο φυσικών αριθμών α και β αλλά δεν διαιρεί ούτε τον α ούτε τον β. Έστω $\alpha = \prod_i p_i$ και $\beta = \prod_j q_j$ οι μοναδικές αναλύσεις σε γινόμενο πρώτων των α και β. Οπότε $p \neq p_i \neq q_j \neq p$ για κάθε i και j. Αλλά τότε $\alpha\beta = \prod_{i,j} p_i q_j$ όπου το p δεν εμφανίζεται στην ανάλυση του $\alpha\beta$ σε γινόμενο πρώτων. Έχουμε όμως ότι $\alpha\beta = p\gamma$, $\gamma \in \mathbb{N}$, και αναλύοντας το γ σε γινόμενο πρώτων, ο p εμφανίζεται στην ανάλυση του $\alpha\beta$ σε γινόμενο πρώτων. Αυτό είναι άτοπο σύμφωνα με το Θεώρημα 1.5.6.

3. Υπάρχουν πολλά παραδείγματα "δακτυλίων" στην άλγεβρα που δεν ικανοποιούν το θεώρημα της μοναδικής παραγοντοποίησης. Επειδή εδώ δεν έχουμε αναφερθεί σε δακτυλίους, θα δώσουμε το πιο απλό παράδειγμα. Θεωρώντας τους άρτιους ακέραιους $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. Αν $\alpha, \beta \in 2\mathbb{Z}$ θα λέμε ότι $\beta \mid \alpha$ αν υπάρχει $\gamma \in 2\mathbb{Z}$ έτσι ώστε $\alpha = \beta\gamma$. Έτσι $2 \mid 4$ αφού $4 = 2 \cdot 2$, ενώ το 2 δεν διαιρεί τον εαυτό του επειδή το $1 \notin 2\mathbb{Z}$. Ένα στοιχείο $p \in 2\mathbb{Z}$ λέγεται "πρώτος" αν δεν υπάρχουν $\alpha, \beta \in 2\mathbb{Z}$ τέτοια ώστε $p = \alpha\beta$. Για παράδειγμα, το 2, το 6, το 14 είναι "πρώτοι" στο $2\mathbb{Z}$. Παρατηρούμε επίσης ότι, ενώ το 2 διαιρεί το 4, το 2 δεν διαιρεί έναν από τους παράγοντές του, $4 = 2 \cdot 2$. Δηλαδή δεν ισχύει το Λήμμα του Ευκλείδη. Παρατηρούμε επίσης ότι δεν ισχύει το θεώρημα μοναδικής παραγοντοποίησης, καθώς $2 \cdot 18 = 6 \cdot 6$ και οι 2, 6 και 18

είναι "πρώτοι". Απ' την άλλη μεριά κάθε μη μηδενικό θετικό στοιχείο του $2\mathbb{Z}$ αναλύεται (παραγοντοποιείται) σε "πρώτους", καθώς το στοιχείο $2z$ αναλύεται σε πρώτους ακέραιους: $2z = 2^k p_1 \cdots p_s$, όπου $p_1, \ldots, p_s$ είναι περιττοί πρώτοι, οπότε έχουμε $2z = 2 \cdots 2(2p_1 \cdots p_s)$ όπου το 2 και το $2p_1 \cdots p_s$ είναι "πρώτοι" παράγοντες του $2z$.

4. Ένα άλλο παράδειγμα είναι το σύνολο $S = \{3k + 1/k \in \mathbb{N}\}$.

Αν $s_1, s_2 \in S$, τότε και $s_1 s_2 \in S$. Αν $\alpha, \beta \in S$, τότε λέμε ότι ο β διαιρεί τον α αν $\alpha = \beta\gamma$, για κάποιο $\gamma \in S$. Ένα δε στοιχείο $p \in S$ λέγεται S-πρώτος αν $p > 1$ και για $r > 1$, $r \in S$ με $r \mid p$ τότε $r = p$. Για παράδειγμα, οι αριθμοί 4, 7, 10 και 13 είναι S-πρώτοι ενώ ο 1 και ο 16 δεν είναι S-πρώτοι. Κάθε δε πρώτος της μορφής $3\kappa + 1$ είναι S-πρώτος, όπως επίσης το γινόμενο δύο πρώτων της μορφής $3\kappa + 2$ είναι S-πρώτος (αφού $(3\kappa + 2)(3\kappa' + 2) = 3\lambda'' + 1$). Έστω $3\lambda + 1 = p_1 p_2 \cdots p_s$ η ανάλυση σε πρώτους ενός στοιχείου του S Επειδή κάθε πρώτος $\neq 3$ είναι της μορφής $3\kappa + 1$ ή $3\kappa + 2$, κάθε p_i είναι της μορφής $3\kappa + 1$ ή $3\kappa + 2$. Επειδή δε $(3\kappa+1)(3\kappa'+2) = 3\kappa''+2$, στην ανάλυση του $3\lambda+1$ πρέπει να υπάρχουν άρτιο πλήθος πρώτων της μορφής $3\kappa + 2$ που το γινόμενό τους είναι ένας S-πρώτος. Άρα κάθε στοιχείο του S αναλύεται σε γινόμενο S-πρώτων.

Παρατηρούμε όμως ότι

$$100 = 3 \cdot 33 + 1 = 4 \cdot 25 = 10 \cdot 10$$

όπου το 4, το 10 και το 25 είναι S-πρώτοι, που σημαίνει ότι δεν έχουμε μοναδική παραγοντοποίηση.

Τώρα κάνουμε την παραδοχή ότι ο αριθμός $n = 1$ ειναι το "κενό" γινόμενο πρώτων. Αν δε στις αναλύσεις των φυσικών αριθμών σε πρώτους παράγοντες συλλέξουμε τους ίσους πρώτους σε δυνάμεις πρώτων, τότε το 1.5.6 μπορεί να ξαναδιατυπωθεί ως εξής.

1.5.7 Θεώρημα. *Κάθε φυσικός αριθμός $n > 0$ γράφεται μοναδικά στη μορφή*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\kappa^{\alpha_\kappa}$$

όπου $p_1, p_2, \ldots, p_\kappa$ είναι πρώτοι με $p_1 < p_2 < \cdots < p_\kappa$ και $\alpha_i \geq 0$, $i = 1, 2, \ldots, \kappa$.

Μερικές φορές μας βολεύει να γράφουμε την ανάλυση του n σε γινόμενο πρώτων και ως

$$n = \prod_{p \in P} p^{\alpha_p},$$

όπου P είναι το σύνολο όλων των πρώτων, κάθε $\alpha_p \geq 0$ και μόνο ένα πεπερασμένο πλήθος εκθετών α_p είναι $\neq 0$. (Θα δούμε ότι το P είναι άπειρο σύνολο).

Οι εκθέτες α_p που εμφανίζονται στην προηγούμενη παραγοντοποίηση του n συνήθως συμβολίζονται με $\upsilon_p(n)$ και χαρακτηρίζονται απ' την εξής ιδιότητα

$$\gamma = \upsilon_p(n) \Leftrightarrow p^\gamma \mid n \text{ και } p^{\gamma+1} \nmid n.$$

Για παράδειγμα, έχουμε $600 = 2^3 \cdot 3 \cdot 5^2$, οπότε $\upsilon_2(600) = 3$, $\upsilon_3(600) = 1$, $\upsilon_5(600) = 2$ και $\upsilon_p(600) = 0$, για κάθε πρώτο $p \neq 2, 3, 5$.

Είναι φανερό ότι κάθε $n \in \mathbb{N}$ ορίζεται μοναδικά από τους εκθέτες $\upsilon_p(n)$.

Η απεικόνιση $\upsilon_p : \mathbb{N} \to \mathbb{N}$ έχει τις εξής ιδιότητες.

1.5.8 Πρόταση. *Για κάθε $m, n \in \mathbb{N}, m, n \geq 1$, ισχύουν τα εξής:*

i) $\upsilon_p(n) = 0$, *για κάθε πρώτο p αν και μόνον αν* $n = 1$

ii) $\upsilon_p(mn) = \upsilon_p(m) + \upsilon_p(n)$

iii) $m \mid n$ *αν και μόνον αν* $\upsilon_p(m) \leq \upsilon_p(n)$, *για κάθε πρώτο p. Συνεπώς η ισότητα ισχύει αν και μόνον αν* $m = n$

iv) $\delta = (m, n)$ *αν και μόνον αν* $\upsilon_p(\delta) = \min\{\upsilon_p(n), \upsilon_p(m)\}$, *για κάθε πρώτο p*

v) $\varepsilon = [m, n]$ *αν και μόνον αν* $\upsilon_p(\varepsilon) = \max\{\upsilon_p(n), \upsilon_p(m)\}$ *για κάθε πρώτο p.*

Απόδειξη. Αποδεικνύουμε την iv), οι υπόλοιπες αφήνονται ως ασκήσεις. Έστω $\delta_p = \min\{\upsilon_p(m), \upsilon_p(n)\}$. Για κάθε p πρώτο, έχουμε $p^{\delta_p} \mid m$ και $p^{\delta_p} \mid n$. Άρα $p^{\delta_p} \mid (m, n)$. Οπότε $\prod p^{\delta_p} \mid (m, n)$. Αν ήταν $1 < \alpha = \dfrac{(m, n)}{\prod p^{\delta_p}}$, τότε $\alpha \mid (m, n)$ και αν p είναι ένας πρώτος διαιρέτης του α τότε $p \mid m$

και $p \mid n$. Αυτό σημαίνει ότι $p^{\delta_p+1} \mid (m,n)$. Αλλά τότε $p^{\upsilon_p(n)+1} \mid n$ και $p^{\upsilon_p(m)+1} \mid m$ που είναι αδύνατον. Άρα $\alpha = 1$. □

Σημειώνουμε ότι η ιδιότητα 1.5.8 ii) είναι η ίδια μ' αυτή που ισχύει στους λογάριθμους.

Προφανώς οι μόνες δυνάμεις του p που διαιρούν τον φυσικό n είναι οι $p^0, p^1, p^2, \ldots, p^{\upsilon_p(n)}$ που είναι σε πλήθος $\upsilon_p(n)+1$. Απ' την 1.5.8 iii) ένας θετικός διαιρέτης του n έχει τη μορφή $p_1^{k_1} \cdots p_s^{k_s}$, $0 \le k_i \le \upsilon_{p_i}(n)$. Οπότε το πλήθος των διαιρετών του n είναι ίσο με

$$\tau(n) = \prod_{p \in P} (\upsilon_p(n) + 1).$$

Εύκολα προκύπτει ότι αν $(m,n) = 1$ για $m, n \in \mathbb{N}$, τότε η συνάρτηση $\tau = \mathbb{N} \to \mathbb{N}$ έχει την ιδιότητα $\tau(nm) = \tau(n)\tau(m)$. Συναρτήσεις που πληρούν αυτή την ιδιότητα ονομάζονται ***πολλαπλασιαστικές συναρτήσεις***.

Η παραγοντοποίηση των θετικών ακεραίων σε πρώτους μπορεί να επεκταθεί και στους αρνητικούς ακεραίους θέτοντας ± 1 εμπρός από το γινόμενο. Επίσης μπορεί να επεκταθεί και στους μη μηδενικούς ρητούς, επιτρέποντας οι εκθέτες να είναι αρνητικοί. Έτσι μπορούμε να επεκτείνουμε την απεικόνιση υ_p στο $\mathbb{Q} - \{0\}$, θέτοντας

$$\upsilon_p(-n) = \upsilon_p(n) \quad \text{για} \quad n \in \mathbb{N}, \quad n \neq 0$$

και

$$\upsilon_p\left(\frac{n}{m}\right) = \upsilon_p(n) - \upsilon_p(m) \quad \text{για} \quad \frac{n}{m} \neq 0.$$

Πρέπει βέβαια να ελέγξουμε αν η υ_p είναι καλά ορισμένη, δηλαδή ότι ο ορισμός της δεν εξαρτάται απ' την εκλογή του αντιπροσώπου του κλάσματος $\dfrac{n}{m}$. Άλλα πράγματι δεν εξαρτάται, αφού έχουμε

$$\begin{aligned} \upsilon_p\left(\frac{n\lambda}{m\lambda}\right) &= \upsilon_p(n\lambda) - \upsilon_p(m\lambda) \\ &= \upsilon_p(n) + \upsilon_p(\lambda) - \upsilon_p(m) - \upsilon_p(\lambda) \\ &= \upsilon_p\left(\frac{n}{m}\right). \end{aligned}$$

Άρα ορίζεται η απεικόνιση

$$\upsilon_p : \mathbb{Q} - \{0\} \to \mathbb{Z}.$$

Έτσι, για παράδειγμα, μπορούμε με την υ_p να καθορίζουμε αν ένας ρητός x είναι ακέραιος: ο x είναι ακέραιος αν και μόνον αν $\upsilon_p(x) \geq 0$, για κάθε πρώτο p. Συνήθως υποθέτουμε ότι $\upsilon_p(0) = \infty$, καθώς κάθε p^{α_p} διαιρεί το μηδέν έχουμε την απεικόνιση

$$\upsilon_p : \mathbb{Q} \to \mathbb{Z}.$$

1.5.9 Θεώρημα. *Κάθε μη-μηδενικός ρητός αριθμός α εκφράζεται μοναδικά στη μορφή*

$$\alpha = \pm \prod_{p \in P} p^{\upsilon_p(\alpha)}$$

όπου P είναι το σύνολο των πρώτων αριθμών.

Άμεσα παίρνουμε

1.5.10 Πόρισμα. *Έστω $\alpha, \beta \in \mathbb{Q} - \{0\}$.*

(i) $\alpha = \pm\beta$ *αν και μόνον αν* $\upsilon_p(\alpha) = \upsilon_p(\beta)$, $\forall\, p \in P$.

(ii) $\alpha = \pm 1$ *αν και μόνον αν* $\upsilon_p(\alpha) = 0$, $\forall\, p \in P$.

Η επόμενη πρόταση αφορά τους ρητούς και είναι η αντίστοιχη της 1.5.8.

1.5.11 Πρόταση. *Έστω p πρώτος και $\alpha, \beta \in \mathbb{Q}$. Τότε*

(i) $\upsilon_p(\alpha\beta) = \upsilon_p(\alpha) + \upsilon_p(\beta)$

(ii) $\upsilon_p(\alpha + \beta) \geq \min\{\upsilon_p(\alpha), \upsilon_p(\beta)\}$. *Η ισότητα ισχύει αν* $\upsilon_p(\alpha) \neq \upsilon_p(\beta)$.

Απόδειξη. (i) Κάθε ρητός α μπορεί να γραφεί ως

$$\alpha = p^{\upsilon_p(\alpha)} \frac{m}{n}$$

όπου $p \nmid m$, $p \nmid n$, $m, n \in \mathbb{Z}$. Απ' αυτό η ιδιότητα i) προκύπτει άμεσα.

ii) Έστω $\alpha = p^u \dfrac{m}{n}$ και $\beta = p^v \dfrac{s}{t}$ όπου p δεν διαιρεί τα m, n, s και t. Εδώ έχουμε $n = \upsilon_p(\alpha)$ και $\upsilon = \upsilon_p(\beta)$.

Έστω ότι $u \leq v$. Τότε

$$\alpha + \beta = p^u \left(\frac{m}{n} + p^{v-u} \frac{s}{t} \right) = p^u \frac{mt + p^{v-u} ns}{nt}.$$

Σημειώνουμε ότι $p \nmid nt$. Δεν γνωρίζουμε όμως αν ο p διαιρεί τον $mt + p^{v-u} ns$. Έστω ότι $mt + p^{v-u} ns = p^\omega k$ όπου $p \nmid k$ και $\omega \geq 0$. Άρα

$$\alpha + \beta = p^{u+\omega} \frac{k}{nt}.$$

Συνεπώς

$$v_p(\alpha + \beta) = u + \omega \geq u = \min(u, v) = \min(v_p(\alpha), v_p(\beta)).$$

Τώρα υποθέτουμε ότι $v_p(\alpha) \neq v_p(\beta)$, δηλαδή $u \neq v$, οπότε $u < v$, δηλαδή $v - u > 0$. Τώρα, αν $p \mid mt + p^{v-u} ns$, τότε $p \mid mt$, αλλά αυτό είναι αδύνατον γιατί $p \nmid m$ και $p \nmid t$. Συνεπώς πρέπει $p \nmid mt + p^{v-u} ns$ που σημαίνει ότι $\omega = 0$. Άρα

$$v_p(\alpha + \beta) = u + \omega = u = \min(u, v) = \min(v_p(\alpha), v_p(\beta)). \qquad \square$$

☞ **1.5.12 Παράδειγμα. 1.** Στο Παράδειγμα 4 του 1.3.11 είχαμε δει ότι, αν μια δύναμη ενός ρητού αριθμού είναι ακέραιος, τότε αυτός ο ρητός είναι ακέραιος. Με την εφαρμογή της απεικόνισης v_p αυτό το αποτέλεσμα προκύπτει άμεσα.

Έστω ότι $\left(\frac{\alpha}{\beta}\right)^n \in \mathbb{Z}$, δηλαδή $\beta^n \mid \alpha^n$. Τότε έχουμε

$$v_p\left(\frac{\alpha^n}{\beta^n}\right) = v_p(\alpha^n) - v_p(\beta^n) = n(v_p(\alpha) - v_p(\beta)) \geq 0$$

ή $v_p(\alpha) - v_p(\beta) \geq 0 \Leftrightarrow \frac{\alpha}{\beta} \in \mathbb{Z}$.

2. Χρησιμοποιώντας το Πόρισμα 1.3.9 είχαμε δείξει στο Παράδειγμα 2 του 1.3.11 ότι ο πραγματικός αριθμός $\sqrt{2}$ είναι άρρητος. Το αποτέλεσμα αυτό μπορεί τώρα να δειχθεί χρησιμοποιώντας το θεμελιώδες θεώρημα της αριθμητικής. Έστω $\sqrt{2} = \frac{\alpha}{\beta}$, όπου $(\alpha, \beta) = 1$, $\alpha, \beta \in \mathbb{N}$. Τότε $2\beta^2 = \alpha^2$. Αν $\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ και $\beta = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$, τότε ο α^2 και ο β^2 αναλύονται σε άρτιο πλήθος πρώτων παραγόντων, ενώ ο $2\beta^2$ σε περιττό.

Άρα δεν μπορεί να ισχύει $2\beta^2 = \alpha^2$. (Απ' αυτό μπορούμε να πάρουμε πολλούς άρρητους ως εξής: Υποθέτουμε $n \in \mathbb{N}$ και $k^2 < n < (k+1)^2$, για κάποιο $k \in \mathbb{N}$. Οπότε $k < \sqrt{n} < k+1$. Άρα ο $\sqrt{n}$ δεν μπορεί να είναι ακέραιος, άρα είναι άρρητος). Με τον ίδιο ισχυρισμό αποδεικνύεται ότι, για κάθε πρώτο p και άρτιο n ο αριθμός $\sqrt[n]{p}$ είναι άρρητος. Αλλά επίσης και αυτό περιλαμβάνεται ως ειδική περίπτωση του εξής γενικού αποτελέσματος. Αν ο $\alpha \in \mathbb{N}$, δεν είναι η n-οστή δύναμη ενός φυσικού αριθμού, για κάποιο $n \in \mathbb{N}$ (δηλαδή, αν ο $\sqrt[n]{\alpha}$ δεν είναι φυσικός), τότε ο $\sqrt[n]{\alpha}$ είναι άρρητος. Πράγματι, υποθέτοντας ότι είναι ρητός, έστω $\sqrt[n]{\alpha} = \dfrac{m}{n}$, $(m,n) = 1$, τότε $\alpha = \dfrac{m^\kappa}{n^\kappa}$ ή $\alpha n^\kappa = m^\kappa$. Οπότε εφαρμόζοντας την απεικόνιση υ_p έχουμε $\kappa\upsilon_p(m) = \upsilon_p(\alpha) + \kappa\upsilon_p(n)$. Συνεπώς $\upsilon_p(n) \le \upsilon_p(m)$. Άρα, λόγω της 1.5.8 iii), πρέπει $n \mid m$ που είναι άτοπο. Εφαρμόζοντας το ίδιο επιχείρημα δείχνουμε ότι, αν r είναι ένας ρητός που δεν είναι ακέραιος, τότε ο αριθμός r^r είναι άρρητος. Πράγματι, έστω $r = \dfrac{\alpha}{\beta}$, $\beta > 1$, $(\alpha,\beta) = 1$. Υποθέτουμε ότι $\left(\dfrac{\alpha}{\beta}\right)^{\frac{\alpha}{\beta}} = \dfrac{\gamma}{\delta}$, $(\gamma,\delta) = 1$, δηλαδή $\left(\dfrac{\alpha}{\beta}\right)^{\alpha} = \left(\dfrac{\gamma}{\delta}\right)^{\beta}$ ή $\alpha^\alpha\delta^\beta = \beta^\alpha\gamma^\beta$. Επειδή $\beta > 1$, υπάρχει ένας πρώτος p που διαιρεί το β, δηλαδή $\upsilon_p(\beta) \neq 0$ και $\upsilon_p(\alpha) = 0$. Έχουμε $\upsilon_p(\alpha^\alpha\delta^\beta) = \upsilon_p(\beta^\alpha\gamma^\beta)$ ή $\alpha\upsilon_p(\alpha) + \beta\upsilon_p(\delta) = \alpha\upsilon_p(\beta) + \beta\upsilon_p(\gamma)$ ή $\beta\upsilon_p(\delta) = \alpha\upsilon_p(\beta) + \beta\upsilon_p(\gamma)$. Επειδή $p \mid \beta^\alpha$ και $p \nmid \alpha^\alpha$ θα πρέπει $p \mid \delta$ και άρα $p \nmid \gamma$. Οπότε έχουμε $\beta\upsilon_p(\delta) = \alpha\upsilon_p(\beta)$. Επειδή $(\alpha,\beta) = 1$, θα πρέπει $\beta \mid \upsilon_p(\beta)$, δηλαδή $\upsilon_p(\beta) = \beta k$, δηλαδή $p^{\beta k} \mid \beta$, οπότε $p^\beta \mid \beta$ που είναι αδύνατο, αφού $\beta < p^\beta$ (πάντα ισχύει $m < n^m$, $m,n \in \mathbb{N}$, $n > 1$, αφού $m = 1 + \cdots + 1 < 1 + n + \cdots + n^{m-1} = \dfrac{n^m - 1}{n-1} \le n^m - 1 < n^m$).

3. Έστω $\alpha,\beta \in \mathbb{N}$ με $\alpha\beta = \gamma^2$, για κάποιο $\gamma \in \mathbb{N}$. Τότε υπάρχουν $\gamma_1,\gamma_2 \in \mathbb{N}$ έτσι ώστε

$$\frac{\alpha}{(\alpha,\beta)} = \gamma_1^2 \quad \text{και} \quad \frac{\beta}{(\alpha,\beta)} = \gamma_2^2.$$

Πράγματι, έστω $\dfrac{\alpha}{(\alpha,\beta)} = p_1^{\alpha_1}\cdots p_s^{\alpha_2}$ και $\dfrac{\beta}{(\alpha,\beta)} = q_1^{\beta_1}\cdots q_\kappa^{\beta_\kappa}$ οι αναλύσεις σε πρώτους. Επειδή ο $\dfrac{\alpha}{(\alpha,\beta)}$ είναι σχετικά πρώτος προς τον $\dfrac{\beta}{(\alpha,\beta)}$ τα σύνολα $\{p_1,\ldots,p_s\}$ και $\{q_1,\ldots,q_\kappa\}$ είναι ξένα μεταξύ τους. Έχουμε δε

$p_1^{\alpha_1}\cdots p_s^{\alpha_s}q_1^{\beta_1}\cdots q_\kappa^{\beta_\kappa}=\left(\dfrac{\gamma}{(\alpha,\beta)}\right)^2$, οπότε τα α_i και β_i πρέπει να είναι άρτιοι αριθμοί και συνεπώς οι $\dfrac{\alpha}{(\alpha,\beta)}$ και $\dfrac{\beta}{(\alpha,\beta)}$ είναι τετράγωνα ακεραίων.

Απ' το 1.3.10 x) προκύπτει ότι αν $(\alpha,\beta)=1$, τότε $\alpha=\gamma_1^2=(\alpha,\beta)^2$ και $\beta=\gamma_2^2=(\beta,\gamma)^2$.

Γενικά ισχύει:

Έστω α,β,γ μη μηδενικοί ακέραιοι, τέτοιοι ώστε $\alpha\beta=\gamma^n$, $(\alpha,\beta)=1$ όπου n είναι ένας θετικός ακέραιος. Τότε $\alpha=\pm\gamma_1^n$ και $\beta=\pm\gamma_2^n$ όπου $\gamma_1,\gamma_2\in\mathbb{Z}$. Επιπλέον, αν n είναι περιττός, τότε $\alpha=\gamma_1^n$ και $\beta=\gamma_2^n$.

Πράγματι, απ' το Θεμελιώδες Θεώρημα της Αριθμητικής, έστω

$$\alpha=\pm p_1^{\alpha_1}\cdots p_s^{\alpha_s}\quad\text{και}\quad\beta=\pm q_1^{\beta_1}\cdots q_k^{\beta_k}$$

οι μοναδικές παραγοντοποιήσεις των α και β σε πρώτους. Επειδή $(\alpha,\beta)=1$, οι πρώτοι p_i είναι όλοι διάφοροι των πρώτων q_j. Επίσης έχουμε $\gamma=\pm p_1^{\gamma_1}\cdots p_s^{\gamma_s}q_1^{\gamma'_1}\cdots q_k^{\gamma'_k}$ αφού $p_i\mid\gamma$ και $q_j\mid\gamma$. Άρα

$$p_1^{\alpha_1}\cdots p_s^{\alpha_s}q_1^{\beta_1}\cdots q_k^{\beta_k}=\pm p_1^{n\gamma_1}\cdots p_s^{n\gamma_s}q_1^{n\gamma'_1}\cdots q_k^{n\gamma'_k}.$$

Συνεπώς απ' τη μοναδική παραγοντοποίηση σε πρώτους προκύπτει ότι

$$\alpha_i=n\gamma_i\quad\text{και}\quad\beta_j=n\gamma'_j.$$

Άρα

$$\alpha=\pm(p_1^{\gamma_1}\cdots p_s^{\gamma_s})^n\quad\text{και}\quad\beta=\pm(q_1^{\gamma'_1}\cdots q_k^{\gamma'_k})^n.$$

Αν ο n είναι περιττός, τότε τα πρόσημα $\pm$ μπορούν να μπουν μέσα στις παρενθέσεις.

4. Το γινόμενο τριών διαδοχικών φυσικών αριθμών δεν μπορεί να είναι μια δύναμη ενός φυσικού αριθμού. Πράγματι, έστω ότι ο ακέραιος $(n-1)n(n+1)=(n^2-1)n$ είναι η m-οστή δύναμη ενός ακεραίου. Αλλά το n^2-1 και το n είναι σχετικά πρώτοι αριθμοί. Από το θεμελιώδες θεώρημα της Αριθμητικής θα πρέπει τότε το n^2-1 και το n^2 να είναι m-οστές δυνάμεις ακεραίων (γιατί;). Επειδή όμως το n^2-1 και το n^2 είναι διαδοχικοί αυτό δεν μπορεί να ισχύει (γιατί;).

5. Αν $\alpha,\beta\in\mathbb{N}$ τέτοιοι ώστε $\alpha\mid\beta^2,\beta^2\mid\alpha^3,\alpha^3\mid\beta^4,\beta^4\mid\alpha^5,\ldots$. Τότε

$\alpha = \beta$. Έστω ότι

$$\alpha = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \quad \text{και} \quad \beta = q_1^{\beta_1} \cdots q_t^{\beta_t}$$

οι αναλύσεις των α και β σε πρώτους. Μας δίνεται ότι για $n = 1, 2, \ldots$ ισχύει

$$p_1^{(2n-1)\alpha_1} \cdots p_s^{(2n-1)\alpha_s} \mid q_1^{2n\beta_1} \cdots q_t^{2n\beta_t}$$

και

$$q_1^{2n\beta_1} \cdots q_t^{2n\beta_t} \mid p_1^{(2n+1)\alpha_1} \cdots p_s^{(2n+1)\alpha_s}.$$

Άρα το $p_i \mid \beta$, για $i = 1, \ldots, s$ και $q_j \mid \alpha$, για $j = 1, \ldots, t$. Οπότε $s = t$ και με μια κατάλληλη αρίθμηση των δεικτών έχουμε $p_i = q_i$, $i = 1, \ldots, s$.

Άρα $\alpha_i \leq \dfrac{2n}{2n-1}\beta_i$ και $\beta_i \leq \dfrac{2n+1}{2n}\alpha_i$. Συνεπώς $\alpha_i - \beta_i \leq \dfrac{\beta_i}{2n-1}$ και $\beta_i - \alpha_i \leq \dfrac{\alpha_i}{2n}$. Καθώς $n \to \infty$ προκύπτει ότι $\alpha_i = \beta_i$.

6. Τα αθροίσματα $H_n = 1 + \dfrac{1}{2} + \dfrac{1}{3} + \cdots + \dfrac{1}{n}$ ονομάζονται ***αρμονικά αθροίσματα***. Έχουμε $H_1 = 1$, $H_2 = \dfrac{3}{2}$, $H_3 = \dfrac{11}{6}$, $H_4 = \dfrac{25}{12}$, $H_5 = \dfrac{137}{60}$, $H_6 = \dfrac{49}{20}, \ldots$. Θα δείξουμε ότι, για $n > 1$, το αρμονικό άθροισμα $H_n = \dfrac{\alpha}{\beta} \notin \mathbb{Z}$ και ότι ο α είναι περιττός και ο β άρτιος. Έστω 2^r η μεγαλύτερη δύναμη του 2 που ανήκει στο σύνολο $S = \{1, 2, \ldots, n\}$. Τότε η δύναμη 2^r δεν διαιρεί κανέναν άλλον αριθμό του S, διότι διαφορετικά αυτός θα ήταν της μορφής $2^r\lambda$ για κάποιο περιττό λ, αλλά τότε και ο αριθμός 2^{r+1} θα ήταν στο S, που είναι αδύνατον αφού $2^{r+1} > n$.

Έστω ε το ε.κ.π. $\{1, 2, \ldots, n\}$. Είναι $\varepsilon = k\alpha_k$, $\alpha_k \in \mathbb{Z}^+$, $1 \leq k \leq n$, $\dfrac{1}{k} = \dfrac{\alpha_k}{\varepsilon}$. Τότε $H_n = \sum\limits_{k=1}^{n} = \dfrac{\Sigma\alpha_k}{\varepsilon}$. Αφού $n \geq 2$, το ε είναι άρτιος. Θα δείξουμε ότι ο $\Sigma\alpha_k$ είναι περιττός και άρα $H_n \notin \mathbb{Z}$. Έχουμε $\varepsilon = 2^r\beta$ όπου β είναι περιττός και άρα $2^r\beta = k\alpha_k$, $1 \leq k \leq n$. Όταν $k = 2^r$, είναι $\alpha_k = \beta$ και αν $k \neq 2^r$, ο k δεν διαιρείται δια του 2^r οπότε ο α_k είναι άρτιος. Άρα ο αριθμητής $\Sigma\alpha_k$ έχει έναν όρο (στο $k = 2^r$) περιττό και όλους τους άλλους άρτιους. Συνεπώς το συνολικό άθροισμα $\sum \alpha_k$ είναι περιττός, δηλαδή $H_n \notin \mathbb{Z}$ και μάλιστα $\upsilon_2(H_n) = -r$.

Αυτό το αποτέλεσμα προκύπτει άμεσα αν εφαρμόσουμε την ***Αρχή του Bertrand***[7] που αναφέρει ότι, για κάθε φυσικό $n > 1$, υπάρχει ένας πρώτος αριθμός p τέτοιος ώστε $n < p < 2n$. Συνεπώς, αν $n \geq 4$ υπάρχει ένας πρώτος p μεταξύ του $\frac{n}{2}$ και του n. Άρα το $\frac{1}{p}$ εμφανίζεται στο άρθοισμα H_n, αλλά το $\frac{1}{2p}$ δεν εμφανίζεται. Εκτός απ' τον όρο $\frac{1}{p}$, σε κάθε άλλο όρο $\frac{1}{k}$, ο k διαιρείται μόνο από πρώτους μικρότερους του p. Συνεπώς

$$H_n = \frac{1}{p} + \frac{\alpha}{\beta}, \quad \text{όπου } \beta \text{ δεν διαιρείται δια } p.$$

Αν ο H_n ήταν ακέραιος, τότε ο $\dfrac{\beta}{p} + \alpha$ θα ήταν ακέραιος που είναι αδύνατον, αφού $p \nmid \beta$.

1.5.13 Θεώρημα. (***Τύπος των de Polignac - Legendre***). *Έστω n ένας θετικός ακέραιος. Τότε η μεγαλύτερη δύναμη ενός πρώτου p που διαιρεί το παραγοντικό $n!$ είναι ίση με*

$$\upsilon_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right].$$

Δηλαδή, η παραγοντοποίηση του $n!$ σε πρώτους δίδεται απ' τον τύπο

$$n! = \prod_{p \in P} p^{\sum\limits_{k=1}^{\infty} \left[\frac{n}{p^k}\right]}.$$

Απόδειξη. Το άθροισμα στο θεώρημα έχει πεπερασμένο πλήθος μη μηδενικούς όρους, αφού $\left[\dfrac{n}{p^k}\right] = 0$ για $p^k > n$. Επίσης αν $p > n$, τότε $p \nmid n!$ και συνεπώς $\displaystyle\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] = 0$.

Αν $p \leq n$ τότε, όπως έχει αναφερθεί στην Παρατήρηση 6 στο 1.2.7, υπάρχουν ακριβώς $\left[\dfrac{n}{p}\right]$ ακέραιοι στο σύνολο $\{1, 2, 3, \ldots, n\}$ που διαιρούνται δια του p. Αυτοί είναι τα πολλαπλάσια του p:

$$p, 2p, 3p, \ldots, \left[\frac{n}{p}\right]p.$$

[7] Η Αρχή του Bertrand απεδείχθη απ' τον Tchebychef το 1850 και άρα είναι θεώρημα.

Σ' αυτά τα πολλαπλάσια του p υπάρχουν ακριβώς $\left[\frac{n}{p^2}\right]$ πολλαπλάσια του p^2:

$$p^2, 2p^2, 3p^2, \ldots, \left[\frac{n}{p^2}\right]p^2.$$

Συνεπώς στα $\left[\frac{n}{p}\right]$ πολλαπλάσια του p πρέπει να προσθέσουμε και τα $\left[\frac{n}{p^2}\right]$ πολλαπλάσια του p που προέρχονται από κάθε πολλαπλάσιο του p^2, $1 \leq p^2 \leq n$. Για τον ίδιο λόγο, μεταξύ αυτών υπάρχουν $\left[\frac{n}{p^3}\right]$ πολλαπλάσια του p^3:

$$p^3, 2p^3, 3p^3, \ldots, \left[\frac{n}{p^3}\right]p^3.$$

Συνεπώς θα προσθέσουμε άλλα $\left[\frac{n}{p^3}\right]$ πολλαπλάσια του p.

Μετά από ένα πεπερασμένο πλήθος επαναλήψεων αυτού του ισχυρισμού θα τερματίσουμε στα πολλαπλάσια του p^t: $p^t, 2p^t, \ldots, \left[\frac{n}{p^t}\right]p^t$, όπου $t = \left[\frac{\log n}{\log p}\right]$, αφού ο t ως ο μεγαλυτερος ακέραιος που είναι μικρότερος του $\frac{\log n}{\log p}$ είναι ο μεγαλύτερος εκθέτης δύναμης του p που είναι μικρότερη του n: $t \leq \frac{\log n}{\log p} \Leftrightarrow p^t \leq n$.

Συνεπώς το συνολικό πλήθος για το πόσες φορές ο p διαιρεί τον $n!$ είναι

$$\sum_{k=1}^{t} \left[\frac{n}{p^k}\right] = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right].$$

Το ίδιο αποτέλεσμα μπορεί να δειχθεί και με επαγωγή στο n: Για $n < p$ τότε ο p δεν διαιρεί το $n!$ και άρα $\upsilon_p(n!) = 0$ και $\left[\frac{n}{p^k}\right] = 0$. Έστω $n \geq p$ και έστω ότι ισχύει

$$\upsilon_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right].$$

Αν $m \in \mathbb{N}$, $m \leq n+1$, τότε $n+1 = m\left[\frac{n+1}{m}\right] + \upsilon$, $0 \leq \upsilon < m$. Αν $\upsilon = 0$, τότε $n = m\left[\frac{n+1}{m}\right] - 1 + m - m = m\left(\left[\frac{n+1}{m}\right] - 1\right) + (m-1)$, οπότε

$$\left[\frac{n+1}{m}\right] = 1 + \left[\frac{n}{m}\right]$$

Αν $\upsilon \neq 0$, τότε $n = m\left[\dfrac{n+1}{m}\right] + \upsilon - 1$, οπότε

$$\left[\frac{n+1}{m}\right] = \left[\frac{n}{m}\right].$$

Τώρα έχουμε ότι, αν ο p δεν διαιρεί τον $n+1$ τότε $\left[\dfrac{n+1}{p^k}\right] = \left[\dfrac{n}{p^k}\right]$ και συνεπώς $\upsilon_p((n+1)!) = \upsilon_p(n!) = \sum\limits_{k=1}^{\infty}\left[\dfrac{n+1}{p^k}\right]$. Αν ο p διαιρεί τον $n+1$, έστω $\upsilon_p(n+1) = \lambda$ και $n+1 = p^\lambda\gamma$, $p \nmid \gamma$. Έχουμε $\left[\dfrac{n+1}{p^k}\right] = \left[\dfrac{n}{p^k}\right] + 1$ για $k \leq \lambda$ και άρα

$$\sum_{k=1}^{\lambda}\left[\frac{n+1}{p^k}\right] = \sum_{k=1}^{\lambda}\left[\frac{n}{p^k}\right] + 1 = \left(\sum_{k=1}^{\lambda}\left[\frac{n}{p^k}\right]\right) + \lambda.$$

Αλλά $\upsilon_p((n+1)!) = \upsilon_p(n!) + \upsilon_p(n+1) = \upsilon_p(n!) + \lambda$. Συνεπώς ισχύει. □

Για παράδειγμα, έστω $n = 454$, τότε ο εκθέτης της μεγαλυτερης δύναμης του 3 που διαιρεί το 454! ισούται με

$$\left[\frac{454}{3}\right] + \left[\frac{454}{9}\right] + \left[\frac{454}{27}\right] + \left[\frac{454}{81}\right] + \left[\frac{454}{243}\right] = 151 + 50 + 16 + 5 + 1 = 223.$$

Επίσης μπορούμε να εφαρμόσουμε το 1.5.13 σε προβλήματα όπως: να βρεθεί το πλήθος των μηδενικών που υπάρχουν στο τέλος του αριθμού 999!. Δηλαδή να βρεθεί η μεγαλυτερη δύναμη του 10 που διαιρεί τον 999!. Επειδή $10 = 2 \cdot 5$ και επειδή υπάρχουν λιγότερα πολλαπλάσια του 5 από τα πολλαπλάσια του 2 μεταξύ των αριθμών $1, 2, \ldots, 999$ (γιατί;) το ζητούμενο πλήθος των μηδενικών καθορίζεται από τη μεγαλύτερη δύναμη του 5 που διαιρεί τον 999!. Σύμφωνα με το 1.5.13 αυτό το πλήθος είναι:

$$\left[\frac{999}{5}\right] + \left[\frac{999}{5^2}\right] + \left[\frac{999}{5^3}\right] + \left[\frac{999}{5^4}\right] = 199 + 39 + 7 + 1 = 246.$$

Άλλο παράδειγμα: Να βρεθεί ο μεγαλύτερος φυσικός αριθμός n τέτοιος ώστε ο 23^{6+n} διαιρεί το 2000!. Έχουμε ότι $\left[\dfrac{2000}{23}\right] = 86$ και $\left[\dfrac{2000}{23^2}\right] = 3$. Άρα 23^{89} είναι η μεγαλύτερη δύναμη του 23 που διαιρεί το 2000!. Άρα $n = 83$.

Ακόμα ένα άλλο παράδειγμα: Έστω P το γινόμενο των πρώτων 100 περιττών θετικών ακεραίων. Να βρεθεί ο μεγαλύτερος ακέραιος k έτσι ώστε ο 3^k να διαιρεί τον P. Παρατηρούμε ότι το γινόμενο των 100 πρώτων περιττών θετικών ακεραίων μπορεί να γραφεί ως

$$1 \cdot 3 \cdot 5 \cdot 7 \cdots 199 = \frac{1 \cdot 2 \cdots 200}{2 \cdot 4 \cdots 200} = \frac{200!}{2^{100} \cdot 100!}.$$

Η μεγαλύτερη δύναμη του 3 που διαιρεί το 200! είναι

$$\left[\frac{200}{3}\right] + \left[\frac{200}{3^2}\right] + \left[\frac{200}{3^3}\right] + \left[\frac{200}{3^4}\right] = 66 + 22 + 7 + 2 = 97.$$

Η μεγαλύτερη δύναμη του 3 που διαιρεί το 100! είναι

$$\left[\frac{100}{3}\right] + \left[\frac{100}{3^2}\right] + \left[\frac{100}{3^3}\right] + \left[\frac{100}{3^4}\right] = 33 + 11 + 3 + 1 = 48.$$

Άρα $k = 97 - 48 = 49$.

Σημείωση: Αν $x \in \mathbb{R}$, ισχύει $\left[\frac{x}{k}\right] = \left[\frac{[x]}{k}\right]$, $\forall\ k \in \mathbb{N}$. Πράγματι, έστω $[x] = k\pi + \upsilon$, $0 < \upsilon < k$ και $x = [x] + \varepsilon$, $0 \leq \varepsilon < 1$. Ισχύει $\pi = \left[\frac{[x]}{k}\right]$ και $\left[\frac{x}{k}\right] = \left[\pi + \frac{\upsilon}{k} + \frac{\varepsilon}{k}\right]$. Απ' αυτό προκύπτει:

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] = \left[\frac{n}{p}\right] + \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + \left[\frac{\left[\frac{\left[\frac{n}{p}\right]}{p}\right]}{p}\right] + \cdots .$$

Αυτή η ισότητα μας διευκολύνει στους υπολογισμούς.

■ **Εφαρμογές:** **1.** Να δειχθεί ότι αν p είναι ένας πρώτος αριθμός και ο p^m διαιρεί το παραγοντικό $n!$ ενός φυσικού αριθμού n τότε $m < n/p - 1$. Πράγματι, θεωρούμε την παράσταση του n ως προς τη βάση p: $n = \alpha_r p^r + \cdots + \alpha_0$, $0 \leq \alpha_i < p$.

2. Γνωρίζουμε από το Θεώρημα 1.5.13 ότι η μεγαλύτερη δύναμη του p που διαιρεί το $n!$ είναι $p^{\sum_{\kappa=1}^{\infty} [\frac{n}{p^\kappa}]}$.

Θέτουμε $\alpha = \sum_{\kappa=1}^{\infty} \left[\frac{n}{p^\kappa}\right]$, και αποδεικνύουμε ότι

$$\alpha(p-1) = n - (\alpha_0 + \alpha_1 + \cdots + \alpha_r).$$

Έχουμε

$$\begin{aligned}
\alpha &= \sum_{\kappa=1}^{\infty} \left[\frac{n}{p^\kappa}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^r}\right] \\
&= \alpha_1 + \alpha_2 p + \cdots + \alpha_r p^{r-1} + \alpha_2 + \alpha_3 p + \cdots + \alpha_r p^{r-2} + \cdots + \alpha_r \\
&= \alpha_1 + \alpha_2(p+1) + \alpha_3(p^2+p+1) + \cdots + \alpha_r(p^{r-1} + \cdots + 1) \\
&= \alpha_1 + \alpha_2\frac{p^2-1}{p-1} + \alpha_3\frac{p^3-1}{p-1} + \cdots + \alpha_r\frac{p^r-1}{p-1}.
\end{aligned}$$

Οπότε

$$\alpha(p-1) = \alpha_1(p-1) + \alpha_2(p^2-1) + \cdots + \alpha_r(p^r-1)$$

ή

$$\begin{aligned}
\alpha(p-1) &= \alpha_0 + \alpha_p + \cdots + \alpha_r p^r - (\alpha_0 + \alpha_1 + \cdots + \alpha_r) \\
&= n - (\alpha_0 + \alpha_1 + \cdots + \alpha_r).
\end{aligned}$$

Συνεπώς ισχύει

$$m \le \alpha = \frac{n}{p-1} - \frac{\alpha_0 + \alpha_1 + \cdots + \alpha_r}{p-1}$$

και άρα $m < \dfrac{n}{p-1}$.

3. Γενικά, όταν θέλουμε να καθορίσουμε τη μεγαλύτερη δύναμη ενός πρώτου που διαιρεί αριθμούς που περιέχουν παραγοντικά, τότε εφαρμόζουμε τον προηγούμενο τύπο. Για παράδειγμα, για τον διωνυμικό συντελεστή

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

έχουμε ότι $\upsilon_p\left(\binom{n}{r}\right) = \upsilon_p(n!) - \upsilon_p(r!) - \upsilon_p(n-r)!$.