4 ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

4.1 Η ΜΑΘΗΜΑΤΙΚΗ ΕΠΑΓΩΓΗ

Εισαγωγή

Η Θεωρία Αριθμών, δηλαδή η μελέτη των ιδιοτήτων των θετικών ακεραίων, έθεσε από πολύ νωρίς τους μαθηματικούς μπροστά στο εξής πρόβλημα:
"Κάποια πρόταση αληθεύει για ορισμένες περιπτώσεις ακεραίων. Είναι όμως αδύνατο να εξεταστούν όλες οι ειδικές περιπτώσεις. Πώς μπορούμε να αποδείξουμε ότι αληθεύει γενικά;"
Μια από τις πλέον ισχυρές μεθόδους για τη λύση αυτού του προβλήματος είναι η μέθοδος της μαθηματικής επαγωγής. Ο (ελληνικής καταγωγής) Ιταλός μαθηματικός Francesco Mauroliko (Μαυρόλυκος) απέδειξε το 1557 ότι:

> *"Το άθροισμα ενός πλήθους περιττών σε διαδοχική σειρά, με αφετηρία τη μονάδα, δίνει το τετράγωνο του πλήθους των περιττών."*
>
> [δηλαδή, με σύγχρονο συμβολισμό, $1+3+5+...+(2\nu-1)=\nu^2$].

Για την απόδειξη ο Μαυρόλυκος χρησιμοποίησε την πρόταση

> *"Κάθε τετράγωνο, όταν αυξάνεται με τον επόμενό του στην τάξη περιττό, δίνει το επόμενο στην τάξη τετράγωνο"*.
>
> [δηλαδή την ταυτότητα $\nu^2+(2\nu+1)=(\nu+1)^2$].

Ουσιαστικά έδειξε λοιπόν ότι υπάρχει ένας γενικός τρόπος μετάβασης από μια περίπτωση στην αμέσως επόμενη. Η μέθοδος αυτή διατυπώθηκε με σαφήνεια από τον Blaise Pascal, το 1654, στην πραγματεία του για το αριθμητικό τρίγωνο. Διατυπώνοντας μια ιδιότητα που ισχύει σε όλες τις γραμμές του τριγώνου, ο Pascal έγραψε τα εξής:

> *"Αν η πρόταση αυτή έχει έναν άπειρο αριθμό περιπτώσεων, θα δώσω μια πολύ σύντομη απόδειξη υποθέτοντας δύο λήμματα.*
> *Το πρώτο, που είναι προφανές, είναι ότι αυτή η ιδιότητα ισχύει στη 2η γραμμή.*
> *Το δεύτερο είναι ότι αν αυτή η ιδιότητα ισχύει σε μια τυχαία γραμμή, τότε θα ισχύει απαραίτητα και στην επόμενη γραμμή.*
> *Από αυτό γίνεται φανερό ότι η πρόταση αληθεύει σε κάθε περίπτωση, γιατί η ιδιότητα ισχύει στη 2η γραμμή, λόγω του πρώτου λήμματος. Έτ-*

σι λόγω του δευτέρου λήμματος θα ισχύει και στην 3η γραμμή, άρα και στην 4η κ.ο.κ., μέχρι το άπειρο."

Οι όροι "μαθηματική επαγωγή" ή "τέλεια επαγωγή", καθιερώθηκαν στη διάρκεια του 19ου αιώνα με τις εργασίες των A. de Morgan (1838) και R. Dedekind (1887), για να γίνει διάκριση από την "ατελή επαγωγή" που χρησιμοποιείται στις Φυσικές Επιστήμες.

Αρχή Μαθηματικής Επαγωγής

Ας υποθέσουμε ότι θέλουμε να βρούμε το άθροισμα

$$1+3+5+7+...+(2\nu-1)$$

για οποιοδήποτε θετικό ακέραιο ν.

Υπολογίζουμε το άθροισμα αυτό για μερικές τιμές του ν και έχουμε:

Για $\nu=1$,	$1=1$	$(=1^2)$
Για $\nu=2$,	$1+3=4$	$(=2^2)$
Για $\nu=3$,	$1+3+5=9$	$(=3^2)$
Για $\nu=4$,	$1+3+5+7=16$	$(=4^2)$

Τα μέχρι τώρα αποτελέσματα μας οδηγούν στην εικασία ότι:

$$1+3+5+7+...+(2\nu-1)=\nu^2. \qquad (1)$$

Επειδή το πλήθος των θετικών ακεραίων είναι άπειρο, συνεχίζοντας με τον παραπάνω τρόπο, είναι αδύνατο να αποδείξουμε ότι η (1) ισχύει για όλους τους θετικούς ακεραίους.

Αν όμως μπορούσαμε να δείξουμε ότι όταν αληθεύει ο ισχυρισμός (1) για αυθαίρετο θετικό ακέραιο ν θα αληθεύει και για τον επόμενό του $\nu+1$, τότε ο ισχυρισμός θα ίσχυε για όλους τους θετικούς ακεραίους. Γιατί τότε, αφού ο ισχυρισμός είναι αληθής για $\nu=1$, θα είναι αληθής και για $\nu=1+1=2$, συνεπώς και για $\nu=2+1=3$ και διαδοχικά για κάθε θετικό ακέραιο.

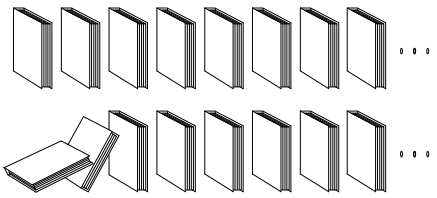
Αν, λοιπόν, υποθέσουμε ότι

$$1+3+5+7+...+(2\nu-1)=\nu^2,$$

τότε θα έχουμε:

$$\begin{aligned}1+3+5+7+...+(2\nu-1)+(2\nu+1) &= [1+3+5+7+...+(2\nu-1)]+(2\nu+1)\\ &= \nu^2+2\nu+1\\ &= (\nu+1)^2.\end{aligned}$$

Αποδείξαμε δηλαδή ότι αν ο ισχυρισμός είναι αληθής για έναν αυθαίρετο θετικό ακέραιο ν, τότε είναι αληθής και για τον επόμενό του ακέραιο $\nu+1$. Άρα, αληθεύει για κάθε θετικό ακέραιο ν.
Μια αναπαράσταση του γεγονότος αυτού είναι η εξής:
Υποθέτουμε ότι έχουμε τοποθετήσει σε μια σειρά ένα πλήθος βιβλίων.



Αν ρίξουμε προς τα πίσω το πρώτο βιβλίο και αν τα βιβλία είναι έτσι τοποθετημένα ώστε κάθε φορά που πέφτει κάποιο βιβλίο να ρίχνει και το επόμενό του, τότε θα ανατραπούν όλα τα βιβλία.
Η αποδεικτική αυτή μέθοδος λέγεται **μαθηματική ή τέλεια επαγωγή** και στηρίζεται στη λεγόμενη "αρχή της μαθηματικής επαγωγής", η οποία διατυπώνεται ως εξής:

ΑΡΧΗ ΤΗΣ ΜΑΘΗΜΑΤΙΚΗΣ ΕΠΑΓΩΓΗΣ

Έστω $P(\nu)$ ένας ισχυρισμός που αναφέρεται στους θετικούς ακεραίους.
Αν
(i) ο ισχυρισμός είναι αληθής για τον ακέραιο 1, δηλαδή ο $P(1)$ είναι αληθής, και
(ii) η αλήθεια του $P(\nu)$ συνεπάγεται την αλήθεια του $P(\nu+1)$ για κάθε ν
τότε ο ισχυρισμός $P(\nu)$ αληθεύει για όλους τους θετικούς ακεραίους ν.

Όπως φαίνεται από τα προηγούμενα, η μέθοδος της μαθηματικής επαγωγής αποτελείται από δύο βήματα. Και τα δύο βήματα είναι απολύτως αναγκαία, για να εξασφαλίσουμε την αλήθεια ενός ισχυρισμού, διότι διαφορετικά μπορεί να οδηγηθούμε σε λάθος συμπεράσματα. Υπάρχουν, δηλαδή, περιπτώσεις στις οποίες ικανοποιείται το 1ο βήμα χωρίς όμως να ικανοποιείται και το 2ο. Για παράδειγμα, το πολυώνυμο $\nu^2-\nu+41$ για $\nu=2$ έχει την τιμή 41, που είναι πρώτος αριθμός, (δηλαδή δεν έχει άλλο διαιρέτη εκτός της μονάδας και του εαυτού του). Αλλά και για $\nu=2,3,4,5,6,7,8,9,10$ έχουμε τις τιμές $43, 47, 53, 61, 71, 83, 97, 113, 131$ αντιστοίχως, που είναι όλοι επίσης πρώτοι αριθμοί. Θα μπορούσε λοιπόν κάποιος να υποθέσει ότι για οποιοδήποτε φυσικό ν η τιμή του πολυώνυμου $\nu^2-\nu+41$ είναι πρώτος αριθμός. Αυτό όμως, ενώ ισχύει μέχρι και $\nu=40$, δεν ισχύει για $\nu=41$, για το οποίο έχουμε $41^2-41+41=41^2$, που δεν είναι πρώτος.

Υπάρχουν επίσης περιπτώσεις στις οποίες ικανοποιείται το 2ο βήμα της μαθηματικής επαγωγής χωρίς όμως να ικανοποιείται και το 1ο. Ας θεωρήσουμε, για παράδειγμα, τον ισχυρισμό:

"Κάθε φυσικός της μορφής $2v$ είναι περιττός".

Αν και ο ισχυρισμός είναι προφανώς ψευδής, ωστόσο ισχύει το 2ο βήμα της μαθηματικής επαγωγής. Πράγματι, αν ο αριθμός $2v$ με v φυσικό είναι περιττός, τότε $2(v+1)=2v+2$ είναι επίσης περιττός, ως άθροισμα του περιττού $2v$ με τον άρτιο 2.

Πολλές φορές πρέπει να αποδείξουμε ότι ένας ισχυρισμός $P(v)$ αληθεύει όχι για κάθε θετικό ακέραιο v αλλά για κάθε v μεγαλύτερο ή ίσο από κάποιο ορισμένο φυσικό αριθμό.

Για παράδειγμα, αν θέλουμε να δείξουμε ότι $2^v > 2v+1$ για κάθε $v \geq 3$, τότε το πρώτο βήμα είναι να αποδείξουμε την αλήθεια της ανισότητας για $v=3$, ενώ αν θέλουμε να αποδείξουμε ότι $3^v \geq 2v+1$ για κάθε $v \geq 0$, τότε το πρώτο βήμα είναι να αποδείξουμε την αλήθεια της ανισότητας για $v=0$.

ΕΦΑΡΜΟΓΕΣ

1. Να αποδειχτεί ότι $1+2+3+...+v=\frac{v(v+1)}{2}$ για κάθε θετικό ακέραιο v.

ΑΠΟΔΕΙΞΗ

Έστω $P(v)$ η ισότητα που θέλουμε να αποδείξουμε.

- Για $v=1$ η ισότητα γίνεται $1=\frac{1(1+1)}{2}$ ή ισοδύναμα 1=1, δηλαδή η $P(1)$ είναι αληθής.
- Θα αποδείξουμε ότι αν $P(v)$ αληθής, τότε και $P(v+1)$ αληθής, δηλαδή ότι:

$$\text{αν } 1+2+3+...+v=\frac{v(v+1)}{2}, \text{ τότε } 1+2+3+...+v+(v+1)=\frac{(v+1)(v+2)}{2}.$$

Έχουμε: $1+2+3+...+v+(v+1)=(1+2+3+...+v)+(v+1)$

$$=\frac{v(v+1)}{2}+(v+1)=(v+1)\left(\frac{v}{2}+1\right)$$

$$=\frac{(v+1)(v+2)}{2}.$$

Άρα, η ισότητα αληθεύει για όλους τους θετικούς ακεραίους v.

2. Να αποδειχτεί ότι για όλους τους θετικούς ακεραίους v με $v \geq 2$ και για όλους τους πραγματικούς α με $\alpha \neq 0$ και $\alpha > -1$ ισχύει: $(1+\alpha)^v > 1+v\alpha$.

(Ανισότητα του Bernoulli)

ΑΠΟΔΕΙΞΗ

Έστω $P(v)$ η ανισότητα που θέλουμε να αποδείξουμε.

- Για $v = 2$ η ανισότητα γίνεται: $(1+a)^2 > 1+2a$, δηλαδή $1+2a+a^2 > 1+2a$ που είναι αληθής, αφού για $a \neq 0$ ισχύει $a^2 > 0$. Ώστε $P(2)$ αληθής.
- Θα αποδείξουμε ότι αν $P(v)$ αληθής, τότε και $P(v+1)$ αληθής, δηλαδή:

$$\text{αν} \quad (1+a)^v > 1+va, \quad \text{τότε} \quad (1+a)^{v+1} > 1+(v+1)a.$$

Έχουμε διαδοχικά:

$$(1+a)^v > 1+va$$

$$(1+a)^v(1+a) > (1+va)(1+a), \qquad \text{αφού} \quad 1+a > 0$$

$$(1+a)^{v+1} > 1+a+va+va^2$$

$$(1+a)^{v+1} > 1+(v+1)a+va^2$$

$$(1+a)^{v+1} > 1+(v+1)a, \qquad \text{αφού} \quad va^2 > 0.$$

Επομένως, η ανισότητα του Bernoulli ισχύει για όλους τους θετικούς ακεραίους v με $v \geq 2$.

ΑΣΚΗΣΕΙΣ

Α΄ ΟΜΑΔΑΣ

1. Να αποδείξετε ότι για κάθε θετικό ακέραιο v ισχύει

(i) $1^2+2^2+3^2+\ldots+v^2 = \dfrac{v(v+1)(2v+1)}{6}$

(ii) $1^3+2^3+3^3+\ldots+v^3 = \left(\dfrac{v(v+1)}{2}\right)^2$

(iii) $1\cdot 2+2\cdot 3+3\cdot 4+\ldots+v(v+1) = \dfrac{v(v+1)(v+2)}{3}$

(iv) $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\dfrac{1}{3\cdot 4}+\ldots+\dfrac{1}{v(v+1)} = \dfrac{v}{v+1}$.

2. Να αποδείξετε ότι για κάθε θετικό ακέραιο v ισχύει

$$1+x+x^2+...+x^{v-1}=\frac{x^v-1}{x-1}, \quad \text{εφόσον} \quad x\neq 1.$$

3. Να αποδείξετε ότι:

(i) $v^2>2v+1$ για κάθε ακέραιο $v\geq 3$

(ii) $\left(\frac{4}{3}\right)^v>v$ για κάθε ακέραιο $v\geq 7$

(iii) $5^v>5v-1$ για κάθε θετικό ακέραιο v.

Β΄ ΟΜΑΔΑΣ

1. Να αποδείξετε ότι για κάθε θετικό ακέραιο $v\geq 4$ ισχύει

$$v!>2^v, \quad \text{όπου} \quad v!=1\cdot 2\cdot 3...v.$$

2. Να αποδείξετε ότι για κάθε θετικό ακέραιο v ισχύει

$$\frac{1}{1^2}+\frac{1}{2^2}+...+\frac{1}{v^2}\leq 2-\frac{1}{v}.$$

3. Να αποδείξετε ότι για κάθε θετικό ακέραιο $v\geq 3$ ισχύει

$$v^{v+1}>(v+1)^v.$$

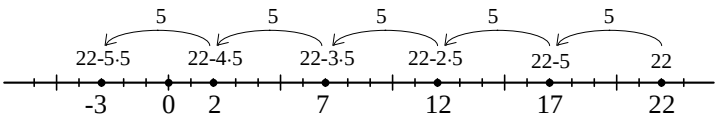
4.2 ΕΥΚΛΕΙΔΕΙΑ ΔΙΑΙΡΕΣΗ

Ας υποθέσουμε ότι θέλουμε να βρούμε το πηλίκο και το υπόλοιπο της διαίρεσης του 22 με τον 5. Σύμφωνα με το γνωστό αλγόριθμο της διαίρεσης, το πηλίκο θα είναι ένας ακέραιος κ, τέτοιος, ώστε:

$$0\leq 22-\kappa\cdot 5<5.$$

Για να βρούμε, λοιπόν, το κ, σχηματίζουμε τις διαφορές:

$$22-5,\quad 22-2\cdot 5,\quad 22-3\cdot 5,\quad 22-4\cdot 5,\quad 22-5\cdot 5,\quad 22-6\cdot 5 \quad \text{κτλ.}$$



Παρατηρούμε ότι αφού οι αριθμοί αυτοί συνεχώς μειώνονται, από ένα σημείο και μετά θα είναι όλοι αρνητικοί. Ο μικρότερος μη αρνητικός ακέραιος από τους παραπάνω αριθμούς, ο οποίος είναι μικρότερος του 5, είναι ο $22-4\cdot 5=2$. Συμπεραίνουμε, λοιπόν, ότι το πηλίκο της διαίρεσης του 22 με τον 5 είναι 4 και το υπόλοιπο 2 και έχουμε:

$$22=4\cdot 5+2,\ 0\le 2<5.$$

Γενικά, ισχύει:

ΘΕΩΡΗΜΑ 1

Αν α και β είναι φυσικοί αριθμοί με $\beta\neq 0$, τότε υπάρχουν μοναδικοί φυσικοί κ και υ, τέτοιοι, ώστε

$$\alpha=\kappa\beta+\upsilon,\ \ 0\le\upsilon<\beta.$$

ΑΠΟΔΕΙΞΗ

- Θεωρούμε τους ακέραιους $\alpha,\alpha-\beta,\alpha-2\beta,\alpha-3\beta,...$ και από αυτούς παίρνουμε τους μη αρνητικούς. Σχηματίζουμε δηλαδή το σύνολο

$$S=\{\alpha-x\beta\,|\,x\in\mathbf{N},\alpha-x\beta\ge 0\}$$

Το σύνολο αυτό είναι υποσύνολο του $\mathbf{N}$ και επιπλέον είναι διάφορο του κενού, αφού περιέχει τον $\alpha-0\cdot\beta=\alpha\ge 0$. Αν υ είναι το ελάχιστο στοιχείο[1] του S, τότε θα υπάρχει $\kappa\in\mathbf{N}$, τέτοιος, ώστε $\upsilon=\alpha-\kappa\beta$, οπότε θα ισχύει

$$\alpha=\kappa\beta+\upsilon\quad\text{και}\quad 0\le\upsilon.$$

Για τον υ πρέπει να δείξουμε ότι είναι και μικρότερος του β. Ας υποθέσουμε λοιπόν ότι $\upsilon\ge\beta$. Τότε

$$\upsilon-\beta\ge 0\ \text{ και }\ \upsilon-\beta=\alpha-\kappa\beta-\beta=\alpha-(\kappa+1)\beta=\alpha-x\beta\ \text{ με }\ x=\kappa+1\in\mathbf{N}.$$

Άρα, ο $\upsilon-\beta$ είναι στοιχείο του συνόλου S, του οποίου ελάχιστο στοιχείο είναι το υ. Έτσι θα ισχύει $\upsilon-\beta\ge\upsilon$, που είναι άτοπο. Επομένως, $\alpha=\kappa\beta+\upsilon,0\le\upsilon<\beta$.

- Μένει τώρα να αποδείξουμε ότι οι φυσικοί αριθμοί κ και υ είναι μοναδικοί. Ας υποθέσουμε ότι και οι φυσικοί κ' και υ' έχουν την ιδιότητα

$$\alpha=\kappa'\beta+\upsilon',\ \ 0\le\upsilon'<\beta.$$

Επειδή $\alpha=\kappa\beta+\upsilon$, $0\le\upsilon<\beta$, θα ισχύει $\kappa'\beta+\upsilon'=\kappa\beta+\upsilon$, οπότε

$$\upsilon-\upsilon'=\beta(\kappa'-\kappa).$$

[1] Αποδεικνύεται ότι κάθε μη κενό υποσύνολο των φυσικών αριθμών έχει ελάχιστο στοιχείο ("αρχή της καλής διάταξης").

Όμως, $0 \le \upsilon < \beta$ και $0 \le \upsilon' < \beta$, οπότε $-\beta < -\upsilon' \le 0$. Επομένως, με πρόσθεση κατά μέλη έχουμε:

$$\begin{aligned} -\beta &< \upsilon - \upsilon' < \beta \\ -\beta &< \beta(\kappa' - \kappa) < \beta \\ -1 &< \kappa' - \kappa < 1 \end{aligned}$$

Αλλά ο μοναδικός ακέραιος μεταξύ -1 και 1 είναι το 0. Άρα $\kappa' - \kappa = 0$, δηλαδή $\kappa' = \kappa$, οπότε και $\upsilon' = \upsilon$. ■

Αποδεικνύεται ότι το θεώρημα ισχύει γενικότερα για οποιουσδήποτε ακέραιους α και β, με $\beta \neq 0$ και διατυπώνεται ως εξής:

Αν α και β ακέραιοι με $\beta \neq 0$, τότε υπάρχουν μοναδικοί ακέραιοι κ και υ, τέτοιοι, ώστε

$$\alpha = \kappa\beta + \upsilon, \quad 0 \le \upsilon < |\beta| .$$

Η διαδικασία εύρεσης των κ, υ λέγεται **ευκλείδεια ή αλγοριθμική διαίρεση** του α με τον β. Το κ λέγεται **πηλίκο** και το υ **υπόλοιπο** της διαίρεσης αυτής. Όταν το υπόλοιπο μιας ευκλείδειας διαίρεσης είναι ίσο με το 0, η διαίρεση λέγεται **τέλεια**.
Ας δούμε με παραδείγματα πώς εργαζόμαστε στις διάφορες περιπτώσεις, για να βρούμε το πηλίκο και το υπόλοιπο μιας ευκλείδειας διαίρεσης.

- Έστω λοιπόν $\alpha = -92$ και $\beta = 5$. Από τη διαίρεση του 92 με τον 5 έχουμε $92 = 5 \cdot 18 + 2$ και επομένως,

$$\begin{aligned} -92 &= -5 \cdot 18 - 2 \\ &= -5 \cdot 18 - 5 + 5 - 2 \\ &= -5 \cdot 19 + 3 \\ &= 5(-19) + 3 . \end{aligned}$$

Άρα, $-92 = 5 \cdot (-19) + 3$, με $0 \le 3 < 5$, που σημαίνει ότι το πηλίκο της διαίρεσης του -92 με τον 5 είναι -19 και το υπόλοιπο είναι 3.

- Έστω τώρα $\alpha = -92$ και $\beta = -5$. Από την ισότητα $92 = 5 \cdot 18 + 2$ έχουμε διαδοχικά

$$\begin{aligned} -92 &= -5 \cdot 18 - 2 \\ &= -5 \cdot 18 - 5 + 5 - 2 \\ &= (-5) \cdot 19 + 3 . \end{aligned}$$

Άρα, $-92 = (-5) \cdot 19 + 3$, με $0 \le 3 < |-5|$, που σημαίνει ότι το πηλίκο της διαίρεσης του -92 με τον -5 είναι 19 και το υπόλοιπο είναι 3.

- Έστω, τέλος, $\alpha=92$ και $\beta=-5$. Πάλι από την ισότητα $92=5\cdot18+2$ έχουμε:

$$92=(-5)\cdot(-18)+2\,,\quad \text{με}\quad 0\le 2<|-5|$$

που σημαίνει ότι το πηλίκο της διαίρεσης του 92 με τον -5 είναι -18 και το υπόλοιπο είναι 2.

ΣΧΟΛΙΟ

Όταν ο διαιρέτης της ευκλείδειας διαίρεσης είναι ο $\beta=2$, τότε τα δυνατά υπόλοιπα είναι $\upsilon=0$ ή $\upsilon=1$.

Αν $\upsilon=0$, ο ακέραιος α έχει τη μορφή $\boldsymbol{\alpha=2\kappa}$, $\kappa\in\mathbf{Z}$ και λέγεται **άρτιος**, ενώ Αν $\upsilon=1$, ο ακέραιος έχει τη μορφή $\boldsymbol{\alpha=2\kappa+1}$, $\kappa\in\mathbf{Z}$ και λέγεται **περιττός**.

Γενικά, τα δυνατά υπόλοιπα του α με τον $\beta>0$ είναι οι αριθμοί

$$0,\ 1,\ 2,\ \ldots,\ \beta-1\,.$$

ΕΦΑΡΜΟΓΕΣ

1. Αν ο α είναι ακέραιος, τότε και ο $\dfrac{\alpha(\alpha^2+2)}{3}$ είναι ακέραιος.

ΑΠΟΔΕΙΞΗ

Επειδή τα δυνατά υπόλοιπα του α με τον 3 είναι 0, 1, 2, ο ακέραιος α έχει μία από τις μορφές $\alpha=3\kappa$ ή $\alpha=3\kappa+1$ ή $\alpha=3\kappa+2$, $\kappa\in\mathbf{Z}$.

- Αν $\alpha=3\kappa$, $\kappa\in\mathbf{Z}$, τότε
$$\frac{\alpha(\alpha^2+2)}{3}=\frac{3\kappa\left[(3\kappa)^2+2\right]}{3}=\kappa(9\kappa^2+2)\in\mathbf{Z}\,.$$
- Αν $\alpha=3\kappa+1$, $\kappa\in\mathbf{Z}$, τότε
$$\frac{\alpha(\alpha^2+2)}{3}=\frac{(3\kappa+1)\left[(3\kappa+1)^2+2\right]}{3}=(3\kappa+1)(3\kappa^2+2\kappa+1)\in\mathbf{Z}\,.$$
- Αν $\alpha=3\kappa+2$, $\kappa\in\mathbf{Z}$, τότε
$$\frac{\alpha(\alpha^2+2)}{3}=\frac{(3\kappa+2)\left[(3\kappa+2)^2+2\right]}{3}=(3\kappa+2)(3\kappa^2+4\kappa+2)\in\mathbf{Z}\,.$$

2. Να αποδειχτεί ότι:

(i) Το γινόμενο δύο διαδοχικών ακεραίων είναι άρτιος αριθμός.

(ii) Το τετράγωνο κάθε περιττού ακεραίου είναι της μορφής $8\lambda+1$, $\lambda\in\mathbf{Z}$.

ΑΠΟΔΕΙΞΗ

(i) Έστω δύο διαδοχικοί ακέραιοι α, $\alpha+1$.

- Αν ο α είναι άρτιος, δηλαδή $\alpha=2\kappa$, $\kappa\in\mathbf{Z}$, τότε

$$\alpha(\alpha+1) = 2\cdot \underbrace{\kappa(2\kappa+1)}_{\lambda} = 2\lambda \text{ , άρτιος.}$$

- Αν ο α είναι περιττός, δηλαδή $\alpha = 2\kappa+1$, $\kappa\in\mathbf{Z}$, τότε

$$\alpha(\alpha+1) = (2\kappa+1)(2\kappa+2) = 2\cdot \underbrace{(2\kappa+1)(\kappa+1)}_{\lambda} = 2\lambda \text{ , άρτιος.}$$

(ii) Έστω ο περιττός $\alpha = 2\kappa+1$, $\kappa\in\mathbf{Z}$. Τότε έχουμε

$$\alpha^2 = (2\kappa+1)^2 = 4\kappa^2+4\kappa+1 = 4\underbrace{\kappa(\kappa+1)}_{2\lambda}+1 = 4\cdot 2\lambda+1 = 8\lambda+1,\ \lambda\in\mathbf{Z}.$$

ΑΣΚΗΣΕΙΣ

Α΄ Ομάδας

1. Να βρείτε το πηλίκο και το υπόλοιπο της ευκλείδειας διαίρεσης του α με τον β σε καθεμιά από τις παρακάτω περιπτώσεις:

(i) $\alpha = 83$ και $\beta = 11$ (ii) $\alpha = -83$ και $\beta = 11$

(iii) $\alpha = 83$ και $\beta = -11$ (iv) $\alpha = -83$ και $\beta = -11$.

2. Να αποδείξετε ότι:
(i) Το τετράγωνο ενός ακεραίου α παίρνει τη μορφή:

$$\alpha^2 = 3\kappa,\ \kappa\in\mathbf{Z} \quad \text{ή} \quad \alpha^2 = 3\kappa+1,\ \kappa\in\mathbf{Z}.$$

(ii) Κάθε ακέραιος α της μορφής $\alpha = 6\kappa+5$, $\kappa\in\mathbf{Z}$ μπορεί να πάρει τη μορφή $\alpha = 3\lambda+2$, $\lambda\in\mathbf{Z}$. Ισχύει το αντίστροφο;

3. Αν α είναι ένας περιττός ακέραιος, να αποδείξετε ότι

$$\frac{\alpha^2+(\alpha+2)^2+(\alpha+4)^2+1}{12}\in\mathbf{Z}.$$

4. Μπορεί ο αριθμός 25 να γραφεί ως άθροισμα 10 προσθετέων, καθένας από τους οποίους να είναι ίσος με 1 ή 3 ή 5;

Β΄ ΟΜΑΔΑΣ

1. Για ποιες τιμές του θετικού ακεραίου β το πηλίκο της διαίρεσης του 660 με τον β είναι ίσο με 17; Ποιο είναι το υπόλοιπο της διαίρεσης αυτής σε καθεμιά περίπτωση;

2. Αν α, β, γ είναι περιττοί ακέραιοι, να αποδείξετε ότι η εξίσωση $\alpha x^2 + \beta x + \gamma = 0$ δεν έχει ακέραιες λύσεις.
Έχει ακέραιες λύσεις η εξίσωση $x^2 + 3^{1997} x + 2001 = 0$;

3. Αν α, β είναι δύο περιττοί ακέραιοι, να αποδείξετε ότι

(i) $\frac{\alpha^2 - \beta^2}{8} \in \mathbf{Z}$ και (ii) $\frac{\alpha^4 + \beta^4 - 2}{16} \in \mathbf{Z}$.

4. Για ποιες τιμές του ακεραίου κ ο αριθμός $\frac{3\kappa + 4}{5}$ είναι ακέραιος;

5. Να αποδείξετε ότι:
(i) Το τετράγωνο ενός άρτιου είναι της μορφής $\alpha^2 = 4\lambda$, $\lambda \in \mathbf{Z}$, ενώ το τετράγωνο ενός περιττού είναι της μορφής $\alpha^2 = 4\lambda + 1$, $\lambda \in \mathbf{Z}$.
(ii) Αν α, β είναι περιττοί ακέραιοι, τότε η εξίσωση $x^2 = \alpha^2 + \beta^2$ δεν έχει ακέραιες ρίζες.
(iii) Κανένας από τους όρους της αριθμητικής προόδου: 6,10,14,18,22,... δεν είναι τετράγωνο φυσικού αριθμού.

4.3 ΔΙΑΙΡΕΤΟΤΗΤΑ

Εισαγωγή

Στα "Στοιχεία" του Ευκλείδη, βιβλία VII, VIII και IX (περίπου 300 π.Χ.), οι θετικοί ακέραιοι παριστάνονται ως ευθύγραμμα τμήματα και η έννοια της διαιρετότητας συνδέεται άμεσα με τη μέτρηση των ευθύγραμμων τμημάτων. Ο Ευκλείδης στην αρχή του βιβλίου VII δίνει 22 ορισμούς, μεταξύ των οποίων και οι εξής:

> Διαιρέτης: *Μέρος εστίν αριθμός αριθμού ο ελάσσων του μείζονος, όταν καταμετρή τον μείζονα.*
> Πολλαπλάσιο: *Πολλαπλάσιος δε ο μείζων του ελάσσονος, όταν καταμετρήται υπό του ελάσσονος.*
> Άρτιος αριθμός: *Άρτιος αριθμός έστιν ο δίχα διαιρούμενος.*
> Περιττός αριθμός: *Περισσός δε ο μη διαιρούμενος δίχα ή ο μονάδι διαφέρων αρτίου αριθμού.*
> Πρώτος αριθμός: *Πρώτος αριθμός έστιν ο μονάδι μόνη μετρούμενος.*

Πρώτοι μεταξύ τους: *Πρώτοι προς αλλήλους αριθμοί εισίν οι μονάδι μετρούμενοι κοινώ μέτρω.*

Τελευταίος δίνεται ο ορισμός του τέλειου αριθμού, δηλαδή αυτού που είναι ίσος με το άθροισμα των γνήσιων διαιρετών του, για παράδειγμα, $28 = 1 + 2 + 4 + 7 + 14$:

Τέλειος αριθμός έστιν ο τοις εαυτού μέρεσιν ίσος ών.

Το ενδιαφέρον των αρχαίων μαθηματικών για τους τέλειους αριθμούς φαίνεται ότι προκλήθηκε από την εξαιρετική σπανιότητά τους. Είναι χαρακτηριστική η παρατήρηση του M. Mersenne (1588-1642) ότι "οι τέλειοι αριθμοί είναι τόσο σπάνιοι όσο και οι τέλειοι άνθρώποι".

Η Θεωρία Αριθμών αρχίζει στο βιβλίο VII με δύο προτάσεις για την εύρεση του μέγιστου κοινού διαιρέτη δύο αριθμών (Ευκλείδειος αλγόριθμος) και ολοκληρώνεται στην τελευταία πρόταση του βιβλίου IX με μια μέθοδο προσδιορισμού τέλειων αριθμών. Με σύγχρονο συμβολισμό, στην πρόταση αυτή ο Ευκλείδης αποδεικνύει ότι:

Αν ο αριθμός $1 + 2 + 2^2 + ... + 2^{v-1} = 2^v - 1$ *είναι πρώτος, τότε ο αριθμός* $2^{v-1}(2^v - 1)$ *είναι τέλειος.*

Έτσι, η γνώση ενός πρώτου αριθμού της μορφής $2^v - 1$ οδηγεί αμέσως στην ανακάλυψη ενός τέλειου αριθμού. Οι πρώτοι 5 αριθμοί αυτού του είδους είναι οι $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$, $2^{13} - 1 = 8191$ και μας δίνουν τους πρώτους 5 τέλειους αριθμούς $6, 28, 496, 8128$ και 33550336. Μέχρι σήμερα έχουν βρεθεί 36 τέλειοι αριθμοί.

Έννοια Διαιρετότητας

Στην ευκλείδεια διαίρεση ιδιαίτερο ενδιαφέρον παρουσιάζει η περίπτωση κατά την οποία το υπόλοιπο είναι ίσο με μηδέν, δηλαδή η περίπτωση της τέλειας διαίρεσης. Την περίπτωση αυτή θα εξετάσουμε στη συνέχεια.

ΟΡΙΣΜΟΣ

Έστω α, β δύο ακέραιοι με $\beta \neq 0$. Θα λέμε ότι ο $\boldsymbol{\beta}$ **διαιρεί τον** $\boldsymbol{\alpha}$ και θα γράφουμε $\boldsymbol{\beta | \alpha}$, όταν η διαίρεση του α με τον β είναι τέλεια, δηλαδή όταν υπάρχει ακέραιος *κ*, τέτοιος, ώστε $\alpha = \kappa\beta$.

Στην περίπτωση αυτή λέμε επίσης ότι ο β είναι **διαιρέτης** ή **παράγοντας** του α ή ότι ο $\boldsymbol{\alpha}$ **διαιρείται με τον** $\boldsymbol{\beta}$ ή ακόμα ότι ο $\boldsymbol{\alpha}$ **είναι πολλαπλάσιο του** $\boldsymbol{\beta}$, και γράφουμε $\boldsymbol{\alpha = \text{πολ}\beta}$.

Για να δηλώσουμε ότι ο ακέραιος β δε διαιρεί τον ακέραιο α, γράφουμε $\beta \nmid a$ ή ισοδύναμα $\alpha \neq \text{πολ}\beta$. Για παράδειγμα, $5 | 20$, αφού $20 = 4 \cdot 5$, ενώ $5 \nmid 18$, αφού η διαίρεση του 18 με τον 5 δεν είναι τέλεια.

Αν $\beta \mid \alpha$, τότε $\alpha = \kappa\beta$ ή ισοδύναμα $\alpha = (-\kappa)(-\beta)$, που σημαίνει ότι αν ο β είναι διαιρέτης του α, τότε και ο $-\beta$ είναι διαιρέτης του α. Επομένως, οι διαιρέτες ενός ακέραιου εμφανίζονται κατά ζεύγη αντίθετων ακέραιων.

Ως άμεσες συνέπειες του παραπάνω ορισμού έχουμε τις εξής:

- $\pm 1 \mid \alpha$ και $\pm \alpha \mid \alpha$ για κάθε $\alpha \in \mathbf{Z}^*$
- $\beta \mid 0$, για κάθε $\beta \in \mathbf{Z}^*$
- Αν $\beta \mid \alpha$, τότε $\kappa\beta \mid \kappa\alpha$, για κάθε $\kappa \in \mathbf{Z}^*$

Τονίζουμε ότι στο συμβολισμό $\beta \mid \alpha$, οι αριθμοί α και β είναι πάντα ακέραιοι και $\beta \neq 0$.

Θα γνωρίσουμε τώρα μερικές χρήσιμες ιδιότητες της διαιρετότητας.

ΘΕΩΡΗΜΑ 2

Έστω α, β, γ ακέραιοι. Ισχύουν οι ακόλουθες ιδιότητες

(i) Αν $\alpha \mid \beta$ και $\beta \mid \alpha$, τότε $\alpha = \beta$ ή $\alpha = -\beta$.

(ii) Αν $\alpha \mid \beta$ και $\beta \mid \gamma$, τότε $\alpha \mid \gamma$.

(iii) Αν $\alpha \mid \beta$, τότε $\alpha \mid \lambda\beta$ για κάθε ακέραιο λ.

(iv) Αν $\alpha \mid \beta$ και $\alpha \mid \gamma$, τότε $\alpha \mid (\beta + \gamma)$.

(v) Αν $\alpha \mid \beta$ και $\beta \neq 0$, τότε $|\alpha| \leq |\beta|$.

ΑΠΟΔΕΙΞΗ

(i) Επειδή $\alpha \mid \beta$ και $\beta \mid \alpha$, υπάρχουν ακέραιοι κ, λ, τέτοιοι, ώστε $\beta = \kappa\alpha$ και $\alpha = \lambda\beta$, οπότε $\alpha = \kappa\lambda\alpha$ και επομένως, $\kappa\lambda = 1$, που σημαίνει ότι $\kappa = \lambda = 1$ ή $\kappa = \lambda = -1$, δηλαδή ότι $\alpha = \beta$ ή $\alpha = -\beta$.

(ii) Επειδή $\alpha \mid \beta$ και $\beta \mid \gamma$, υπάρχουν ακέραιοι κ, λ, τέτοιοι, ώστε $\beta = \kappa\alpha$ και $\gamma = \lambda\beta$, οπότε $\gamma = \lambda\kappa \cdot \alpha$ και άρα $\alpha \mid \gamma$.

(iii) Επειδή $\alpha \mid \beta$ υπάρχει ακέραιος κ, τέτοιος, ώστε $\beta = \kappa\alpha$, οπότε $\lambda\beta = \lambda\kappa \cdot \alpha$ και άρα $\alpha \mid \lambda\beta$.

(iv) Επειδή $\alpha \mid \beta$ και $\alpha \mid \gamma$, υπάρχουν ακέραιοι κ, λ, τέτοιοι, ώστε $\beta = \kappa\alpha$ και $\gamma = \lambda\alpha$, οπότε $\beta + \gamma = (\kappa + \lambda)\alpha$ και άρα $\alpha \mid (\beta + \gamma)$.

(v) Επειδή $\alpha \mid \beta$ και $\beta \neq 0$, υπάρχει ακέραιος $\kappa \neq 0$ με $\beta = \kappa\alpha$. Επομένως, $|\beta| = |\kappa| \cdot |\alpha| \geq |\alpha|$, αφού $|\kappa| \geq 1$. ■

Από τις ιδιότητες (iii) και (iv) του παραπάνω θεωρήματος προκύπτει ότι:

"Αν $\alpha \mid \beta$ και $\alpha \mid \gamma$, τότε $\alpha \mid (\kappa\beta + \lambda\gamma)$ για όλους τους ακεραίους κ και λ."

Ο ακέραιος $\kappa\beta + \lambda\gamma$, όπου $\kappa, \lambda \in \mathbf{Z}$ λέγεται **γραμμικός συνδυασμός** των β και γ.

ΕΦΑΡΜΟΓΕΣ

1. Αν α,δ ακέραιοι με $\delta|(2\alpha+1)$ και $\delta|(3\alpha-1)$, να βρεθούν οι πιθανές θετικές τιμές του δ.

ΛΥΣΗ

Επειδή $\delta|(2\alpha+1)$ και $\delta|(3\alpha-1)$, ο δ διαιρεί και τον $3(2\alpha+1)-2(3\alpha-1)=5$. Αφού λοιπόν $\delta>0$ και $\delta|5$, θα είναι $\delta=1$ ή $\delta=5$.

2. Να αποδειχτεί ότι $9^{\nu+1}-8\nu-9=$ πολ64, για κάθε $\nu\in\mathbf{N}^*$.

ΑΠΟΔΕΙΞΗ

Θα αποδείξουμε την πρόταση με τη μέθοδο της μαθηματικής επαγωγής.

- Η ισότητα ισχύει για $\nu=1$, αφού $9^{1+1}-8\cdot1-9=64=$ πολ8
- Θα αποδείξουμε ότι

$$\text{αν } 9^{\nu+1}-8\nu-9=\text{πολ}64=64\lambda,\ \lambda\in\mathbf{Z},\ \text{τότε}\ \ 9^{\nu+2}-8(\nu+1)-9=\text{πολ}64.$$

Έχουμε:
$$\begin{aligned}9^{\nu+2}-8(\nu+1)-9&=9\cdot9^{\nu+1}-8\nu-17\\&=9(64\lambda+8\nu+9)-8\nu-17\\&=9\lambda\cdot64+72\nu+81-8\nu-17\\&=64(9\lambda+\nu+1)\\&=\text{πολ}64.\end{aligned}$$

Άρα η ισότητα αληθεύει για όλους τους θετικούς ακεραίους.

3. Να αποδειχτεί ότι ο 3 διαιρεί τους ακεραίους α και β, αν και μόνο αν ο 3 διαιρεί το άθροισμα $\alpha^2+\beta^2$.

ΑΠΟΔΕΙΞΗ

- Αν $3|\alpha$ και $3|\beta$, τότε $3|(\alpha\cdot\alpha+\beta\cdot\beta)$, δηλαδή $3|(\alpha^2+\beta^2)$.

- Έστω $3|(\alpha^2+\beta^2)$. Αν $\alpha=3\kappa_1+\upsilon_1$, $0\le\upsilon_1<3$ και $\beta=3\kappa_2+\upsilon_2$, $0\le\upsilon_2<3$ είναι οι ισότητες των αλγοριθμικών διαιρέσεων των α και β με τον 3, τότε

$$\alpha^2=9\kappa_1^2+6\kappa_1\upsilon_1+\upsilon_1^2=3\underbrace{(3\kappa_1^2+2\kappa_1\upsilon_1)}_{\lambda_1}+\upsilon_1^2=3\lambda_1+\upsilon_1^2.$$
$$\beta^2=9\kappa_2^2+6\kappa_2\upsilon_2+\upsilon_2^2=3\underbrace{(3\kappa_2^2+2\kappa_2\upsilon_2)}_{\lambda_2}+\upsilon_2^2=3\lambda_2+\upsilon_2^2.$$

οπότε $\alpha^2+\beta^2=3\lambda+(\upsilon_1^2+\upsilon_2^2)$, όπου $\lambda=\lambda_1+\lambda_2\in\mathbf{Z}$.

Επειδή $3|(\alpha^2+\beta^2)$ και $3|3\lambda$, πρέπει $3|(\upsilon_1^2+\upsilon_2^2)$. Όμως $\upsilon_1, \upsilon_2 \in \{0,1,2\}$ οπότε, για τις τιμές της παράστασης $(\upsilon_1^2+\upsilon_2^2)$, έχουμε τον παρακάτω πίνακα:

υ_2 \ υ_1	**0**	**1**	**2**
0	$\upsilon_1^2+\upsilon_2^2=$**0**	$\upsilon_1^2+\upsilon_2^2=$**1**	$\upsilon_1^2+\upsilon_2^2=$**4**
1	$\upsilon_1^2+\upsilon_2^2=$**1**	$\upsilon_1^2+\upsilon_2^2=$**2**	$\upsilon_1^2+\upsilon_2^2=$**5**
2	$\upsilon_1^2+\upsilon_2^2=$**4**	$\upsilon_1^2+\upsilon_2^2=$**5**	$\upsilon_1^2+\upsilon_2^2=$**8**

Από τον πίνακα αυτόν προκύπτει ότι $3|(\upsilon_1^2+\upsilon_2^2)$, μόνο όταν $\upsilon_1=0$ και $\upsilon_2=0$, δηλαδή μόνο όταν $\alpha=3\kappa_1$ και $\beta=3\kappa_2$, που σημαίνει ότι $3|\alpha$ και $3|\beta$.

ΑΣΚΗΣΕΙΣ

Α΄ ΟΜΑΔΑΣ

1. Να βρείτε το πλήθος των θετικών ακεραίων που δεν υπερβαίνουν τον 1000 και διαιρούνται με:

(i) τον 5, (ii) τον 25, (iii) τον 125, (iv) τον 625.

2. Αν $\alpha|\beta$ και $\gamma|\delta$, να αποδείξετε ότι $\alpha\gamma|\beta\delta$.

3. Αν $11|(\alpha+2)$ και $11|(35-\beta)$, να αποδείξετε ότι $11|(a+\beta)$.

4. Αν η διαφορά δύο ακεραίων είναι άρτιος αριθμός, να αποδείξετε ότι η διαφορά των τετραγώνων τους είναι πολλαπλάσιο του 4.

5. Αν $m|\alpha$ και $m>1$, να αποδείξετε ότι $m\nmid\alpha+1$.

6. Να αποδείξετε ότι $2|(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$ για όλους τους ακέραιους α,β,γ.

Β΄ ΟΜΑΔΑΣ

1. Έστω α ένας περιττός ακέραιος. Να αποδείξετε ότι

(i) Το τετράγωνο του α είναι της μορφής $\alpha^2=4\lambda+1$, $\lambda\in\mathbf{Z}$

(ii) $32|(\alpha^2+3)(\alpha^2+7)$

2. Να αποδείξετε ότι $4\nmid(\alpha^2+2)$, για κάθε $a\in\mathbf{Z}$.

3. Να αποδείξετε ότι δεν υπάρχουν διαδοχικοί θετικοί ακέραιοι που να είναι και οι δύο τετράγωνα ακεραίων.

4. Αν $\beta|a$ να αποδείξετε ότι $(2^\beta-1)|(2^\alpha-1)$.

5. Να αποδείξετε ότι

(i) Το γινόμενο τριών διαδοχικών ακεραίων διαιρείται με το 6.

(ii) $6|\alpha(\alpha+1)(2\alpha+1)$ για κάθε $a\in\mathbf{Z}$

(iii) $6|(\alpha^3+3\alpha^2-4\alpha)$ για κάθε $a\in\mathbf{Z}$.

6. Να αποδείξετε ότι

(i) $3|(\nu^3+2\nu)$ για κάθε $\nu\in\mathbf{N}$

(ii) $64|(9^{\nu+1}-8\nu-9)$ για κάθε $\nu\in\mathbf{N}$

(iii) $5|(3\cdot 27^\nu+2\cdot 2^\nu)$ για κάθε $\nu\in\mathbf{N}$

(iv) $14|(3^{4\nu+2}+5^{2\nu+1})$ για κάθε $\nu\in\mathbf{N}$

7. Έστω $\alpha,\beta,\kappa,\lambda\in\mathbf{Z}$ με $\kappa\neq\lambda$. Αν $(\kappa-\lambda)|(\kappa\alpha+\lambda\beta)$, να αποδείξετε ότι $(\kappa-\lambda)|(\lambda\alpha+\kappa\beta)$.

4.4 ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ - ΕΛΑΧΙΣΤΟ ΚΟΙΝΟ ΠΟΛΛΑΠΛΑΣΙΟ

Μέγιστος Κοινός Διαιρέτης

Έστω α, β δύο ακέραιοι. Ένας ακέραιος δ λέγεται **κοινός διαιρέτης** των α και β, όταν είναι διαιρέτης και του α και του β. Το σύνολο των θετικών κοινών διαιρετών δύο ακεραίων έχει ένα τουλάχιστον στοιχείο, αφού ο 1 είναι πάντα ένας θετικός κοινός διαιρέτης τους. Αν ένας τουλάχιστον από τους δύο ακεραίους είναι διαφορετικός από το 0, τότε το σύνολο των θετικών κοινών

διαιρετών τους είναι πεπερασμένο, και επομένως ανάμεσά τους υπάρχει μέγιστο στοιχείο. Αν όμως και οι δύο ακέραιοι είναι μηδέν, τότε κάθε θετικός ακέραιος είναι κοινός διαιρέτης τους και επομένως το σύνολο των θετικών κοινών διαιρετών τους δεν έχει μέγιστο στοιχείο.

ΟΡΙΣΜΟΣ

Έστω α και β δύο ακέραιοι, από τους οποίους ένας τουλάχιστον είναι διάφορος του μηδενός. Ορίζουμε ως **μέγιστο κοινό διαιρέτη** (Μ.Κ.Δ.) των α και β, και τον συμβολίζουμε με $\boldsymbol{(\alpha,\beta)}$, το μεγαλύτερο[1] από τους θετικούς κοινούς διαιρέτες τους.

Δηλαδή, ο Μ.Κ.Δ. δύο ακεραίων α και β είναι ο μοναδικός *θετικός* ακέραιος δ που έχει τις επόμενες δύο ιδιότητες:

(1) $\delta|\alpha$ και $\delta|\beta$

(2) Αν $x|\alpha$ και $x|\beta$, τότε $x \le \delta$.

Από τον παραπάνω ορισμό προκύπτει ότι

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

Έτσι ,για παράδειγμα, αν $\alpha=-12$ και $\beta=30$, τότε $(-12,30)=(12,30)=6$, αφού οι θετικοί διαιρέτες του 12 είναι οι $1,2,3,4,6,12$, του 30 οι $1,2,3,5,6,10,15,30$ και ο μεγαλύτερος κοινός διαιρέτης τους είναι ο 6.

Παρατηρούμε επίσης ότι:

- Για κάθε $\theta\varepsilon\tau\iota\kappa\acute{o}$ ακέραιο α ισχύει $(\alpha,\alpha)=\alpha$, $(\alpha,0)=\alpha$ και $(\alpha,1)=1$.
- Αν α, β είναι δύο $\theta\varepsilon\tau\iota\kappa o\acute{\iota}$ ακέραιοι με $\beta|\alpha$, τότε $(\alpha,\beta)=\beta$.

Δύο ακέραιοι α και β, που έχουν μέγιστο κοινό διαιρέτη τη μονάδα, για τους οποίους δηλαδή ισχύει $(\alpha,\beta)=1$, λέγονται **πρώτοι μεταξύ τους**. Για παράδειγμα, οι 28 και 15 είναι πρώτοι μεταξύ τους, αφού $(28,15)=1$.

Αν για τον υπολογισμό του Μ.Κ.Δ. δύο ακεραίων προσδιορίζουμε προηγουμένως τους διαιρέτες τους, τότε, ιδιαίτερα για μεγάλους αριθμούς, απαιτείται πολύς χρόνος. Μια σύντομη και αποτελεσματική μέθοδος προσδιορισμού του Μ.Κ.Δ. οφείλεται στον Ευκλείδη και λέγεται **ευκλείδειος αλγόριθμος**. Ο αλγόριθμος αυτός στηρίζεται στο επόμενο θεώρημα.

ΘΕΩΡΗΜΑ 3

Αν α, β είναι δύο φυσικοί αριθμοί και υ είναι το υπόλοιπο της ευκλείδειας διαίρεσης του α με τον β, τότε

[1] Αποδεικνύεται ότι: “Κάθε πεπερασμένο υποσύνολο του **R** έχει μέγιστο στοιχείο”.

$$(\alpha,\beta)=(\beta,\upsilon)\,.$$

ΑΠΟΔΕΙΞΗ

Έστω $\alpha=\kappa\beta+\upsilon$, $0\le\upsilon<\beta$ η ισότητα της ευκλείδειας διαίρεσης του α με τον β. Αν $\delta=(\alpha,\beta)$ και $\delta'=(\beta,\upsilon)$, τότε:

- Επειδή $\delta|\alpha$ και $\delta|\beta$, προκύπτει ότι $\delta|(\alpha-\kappa\beta)$, δηλαδή $\delta|\upsilon$. Έτσι $\delta|\beta$ και $\delta|\upsilon$, άρα $\delta\le\delta'$.

- Επειδή $\delta'|\beta$ και $\delta'|\upsilon$, προκύπτει ότι $\delta'|(\kappa\beta+\upsilon)$, δηλαδή $\delta'|\alpha$. Έτσι $\delta'|\beta$ και $\delta'|\alpha$, άρα $\delta'\le\delta$.

Επομένως, $\delta=\delta'$. ■

Ας χρησιμοποιήσουμε το παραπάνω θεώρημα στον υπολογισμό του Μ.Κ.Δ. των 111 και 78. Εφαρμόζοντας διαδοχικά την ευκλείδεια διαίρεση έχουμε:

$$\begin{aligned}111&=1\cdot78+33\\78&=2\cdot33+12\\33&=2\cdot12+9\\12&=1\cdot9+3\\9&=3\cdot3+0\,.\end{aligned}$$

Επομένως,

$$(111,\,78)=(78,\,33)=(33,\,12)=(12,\,9)=(9,\,3)=(3,\,0)=3\,,$$

δηλαδή $(111,78)=3$, που είναι και το τελευταίο μη μηδενικό υπόλοιπο των διαδοχικών διαιρέσεων.

Γενικά, για δύο θετικούς ακεραίους α, β με $\alpha>\beta$, η διαδικασία μπορεί να περιγραφεί ως εξής: Εφαρμόζουμε επανειλημμένα και διαδοχικά την ευκλείδεια διαίρεση και γράφουμε

$$\begin{aligned}\alpha&=\kappa_1\beta+\upsilon_1\,, &&0<\upsilon_1<\beta\\ \beta&=\kappa_2\upsilon_1+\upsilon_2\,, &&0<\upsilon_2<\upsilon_1\\ \upsilon_1&=\kappa_3\upsilon_2+\upsilon_3\,, &&0<\upsilon_3<\upsilon_2\\ &\cdots\cdots\cdots\cdots\cdots\cdots\end{aligned}$$

Από τον έλεγχο των ανισοτήτων στη δεξιά στήλη βλέπουμε ότι για την ακολουθία των διαδοχικών υπολοίπων ισχύει $\beta>\upsilon_1>\upsilon_2>\upsilon_3>...\ge0$. Επομένως, ύστερα από β το πολύ βήματα θα εμφανιστεί το υπόλοιπο 0. Ας υποθέσουμε λοιπόν ότι

$$\upsilon_{\nu-2}=\kappa_\nu\upsilon_{\nu-1}+\upsilon_\nu,\ \ \upsilon_\nu>0$$

$$\upsilon_{\nu-1} = \kappa_{\nu+1}\upsilon_{\nu} + 0 .$$

Τότε ισχύει $(\alpha,\beta)= \upsilon_{\nu}$. Αυτό προκύπτει από τη διαδοχική εφαρμογή του προηγούμενου θεωρήματος, σύμφωνα με το οποίο

$$\boldsymbol{(\alpha,\beta)=(\beta,\upsilon_1)=(\upsilon_1,\upsilon_2)=...=(\upsilon_{\nu},0)= \upsilon_{\nu}} .$$

Επομένως, ο Μ.Κ.Δ. των α και β είναι **το τελευταίο θετικό υπόλοιπο** των παραπάνω αλγοριθμικών διαίρεσεων.
Η διαδικασία αυτή αποτελεί τον **ευκλείδειο αλγόριθμο** και χρησιμοποιείται γενικότερα για τον προσδιορισμό του Μ.Κ.Δ. δύο οποιωνδήποτε ακεραίων.
Από τον παραπάνω αλγόριθμο μπορεί να προκύψει η πολύ σημαντική ιδιότητα του Μ.Κ.Δ. δύο αριθμών α, β, ότι δηλαδή αυτός μπορεί να εκφραστεί ως γραμμικός συνδυασμός των α και β.

Για παράδειγμα, από τη διαδικασία προσδιορισμού του Μ.Κ.Δ. των α =111 και β =78 έχουμε:

$$33=111-1\cdot 78$$
$$12=78-2\cdot 33$$
$$9=33-2\cdot 12$$
$$3=12-1\cdot 9$$

Επομένως,

$$3=12-1\cdot 9=12-1\cdot(33-2\cdot 12)= -1\cdot 33+3\cdot 12$$
$$= -1\cdot 33+3\cdot(78-2\cdot 33)=3\cdot 78-7\cdot 33$$
$$=3\cdot 78-7\cdot(111-1\cdot 78)=(-7)\cdot 111+10\cdot 78 .$$

Ώστε

$$\boldsymbol{(111,78)=3=(-7)\cdot 111+10\cdot 78} .$$

Γενικά, ισχύει:

ΘΕΩΡΗΜΑ 4

Αν δ είναι ο Μ.Κ.Δ. των α και β, τότε υπάρχουν ακέραιοι κ και λ, τέτοιοι, ώστε

$$\delta = \kappa\alpha + \lambda\beta .$$

Δηλαδή, ο Μ.Κ.Δ. δύο ακέραιων μπορεί να γραφεί ως γραμμικός συνδυασμός των ακεραίων αυτών.

Οι ακέραιοι κ και λ δεν είναι μοναδικοί. Για παράδειγμα για το Μ.Κ.Δ. των 111 και 78 είναι $3=(-7)\cdot 111+10\cdot 78$ αλλά και $3=71\cdot 111+(-101)\cdot 78$.

ΠΟΡΙΣΜΑ 1

Δύο ακέραιοι $\alpha,\ \beta$ είναι πρώτοι μεταξύ τους, αν και μόνο αν υπάρχουν ακέραιοι $\kappa,\ \lambda$, τέτοιοι, ώστε

$$\kappa\alpha+\lambda\beta=1.$$

ΑΠΟΔΕΙΞΗ

- Αν $\alpha,\ \beta$ είναι πρώτοι μεταξύ τους, τότε $(\alpha,\beta)=1$ και επομένως υπάρχουν ακέραιοι $\kappa,\ \lambda$ με $\kappa\alpha+\lambda\beta=1$
- Αν υπάρχουν ακέραιοι $\kappa,\ \lambda$ με $\kappa\alpha+\lambda\beta=1$ και αν $\delta=(\alpha,\beta)$, τότε $\delta|\alpha$ και $\delta|\beta$ και επομένως, $\delta|(\kappa\alpha+\lambda\beta)$, δηλαδή $\delta|1$, οπότε $\delta=1$. ■

Αν $\kappa\alpha+\lambda\beta=\delta$ είναι η γραμμική έκφραση του μέγιστου κοινού διαιρέτη των ακεραίων α και β, τότε $\kappa\left(\frac{\alpha}{\delta}\right)+\lambda\left(\frac{\beta}{\delta}\right)=1$, που σημαίνει ότι $\left(\frac{\alpha}{\delta},\frac{\beta}{\delta}\right)=1$.

Δηλαδή:

“Αν διαιρέσουμε δύο ακέραιους με το Μ.Κ.Δ. τους, προκύπτουν αριθμοί πρώτοι μεταξύ τους”.

ΠΟΡΙΣΜΑ 2

Οι κοινοί διαιρέτες δύο ακεραίων α και β είναι οι διαιρέτες του μέγιστου κοινού διαιρέτη τους.

ΑΠΟΔΕΙΞΗ

Έστω $\delta=(\alpha,\beta)$. Προφανώς κάθε διαιρέτης του δ είναι και κοινός διαιρέτης των α και β. Αλλά και αντιστρόφως, κάθε κοινός διαιρέτης δ' των α και β είναι και διαιρέτης του Μ.Κ.Δ. των α,β. Πράγματι, αν $\kappa\alpha+\lambda\beta=\delta$ είναι η γραμμική έκφραση του δ, τότε $\delta'|(\kappa\alpha+\lambda\beta)$, δηλαδή $\delta'|\delta$. ■

Για παράδειγμα, επειδή $(150,120)=30$, οι θετικοί κοινοί διαιρέτες των 150 και 120 είναι οι διαιρέτες του 30, δηλαδή οι ακέραιοι 1,2,3,5,6,10,15 και 30.

ΠΟΡΙΣΜΑ 3

Αν για τους ακεραίους $\alpha,\ \beta,\ \gamma$ ισχύει $\alpha|\beta\gamma$ και $(\alpha,\beta)=1$, τότε $\alpha|\gamma$.

Δηλαδή, αν ένας ακέραιος διαιρεί το γινόμενο δύο ακεραίων και είναι πρώτος προς τον έναν, τότε διαιρεί τον άλλο.

ΑΠΟΔΕΙΞΗ

Επειδή $(\alpha,\beta)=1$, υπάρχουν ακέραιοι κ, λ, τέτοιοι, ώστε $\kappa\alpha+\lambda\beta=1$ και επομένως $\kappa\alpha\gamma+\lambda\beta\gamma=\gamma$. Αφού $\alpha|\alpha\gamma$ και $\alpha|\beta\gamma$, θα ισχύει $\alpha|(\kappa\alpha\gamma+\lambda\beta\gamma)$, δηλαδή $\alpha|\gamma$. ■

Η συνθήκη $(\alpha,\beta)=1$ είναι αναγκαία, για να ισχύει το θεώρημα. Για παράδειγμα, ενώ $4|2\cdot6$, $4\not|2$ και $4\not|6$.

Η έννοια του μέγιστου κοινού διαιρέτη γενικεύεται και για περισσότερους από δύο ακεραίους. Συγκεκριμένα, αν $\alpha_1,\alpha_2,\alpha_3,...,\alpha_\nu$ ακέραιοι με έναν τουλάχιστον διάφορο του μηδενός, τότε ορίζουμε ως μέγιστο κοινό διαιρέτη αυτών, και τον συμβολίζουμε με $(\alpha_1,\alpha_2,\alpha_3,...,\alpha_\nu)$, τον μεγαλύτερο από τους θετικούς κοινούς διαιρέτες τους. Αποδεικνύεται ότι:

"Ο Μ.Κ.Δ. τριών ή περισσότερων ακεραίων δε μεταβάλλεται αν αντικαταστήσουμε δύο από αυτούς με το μέγιστο κοινό διαιρέτη τους".

Για παράδειγμα $(24,12,16)=((24,16),12)=(8,12)=4$

Για το Μ.Κ.Δ. περισσότερων από δύο ακεραίους ισχύουν ανάλογες ιδιότητες με τις ιδιότητες του Μ.Κ.Δ. δύο ακεραίων. Έτσι ,για παράδειγμα, για τρεις ακέραιους α,β,γ αποδεικνύεται ότι:

- **Αν $\delta=(\alpha,\beta,\gamma)$, τότε υπάρχουν ακέραιοι κ,λ,μ, τέτοιοι, ώστε**

$$\delta=\kappa\alpha+\lambda\beta+\mu\gamma\ .$$

- **Αν $\delta=(\alpha,\beta,\gamma)$, τότε $\left(\frac{\alpha}{\delta},\frac{\beta}{\delta},\frac{\gamma}{\delta}\right)=1$.**

ΕΦΑΡΜΟΓΕΣ

1. Να αποδειχτεί ότι για τους ακεραίους α,β,κ ισχύουν

(i) $(\alpha,\beta)=(\alpha-\kappa\beta,\beta)$

(ii) $(\alpha,\beta)=(\alpha-\beta,\beta)$

(iii) $(\alpha,\alpha+1)=1$.

ΑΠΟΔΕΙΞΗ

(i) Έστω $\delta=(\alpha,\beta)$ και $\delta'=(\alpha-\kappa\beta,\beta)$, τότε

- $\begin{cases}\delta|\alpha\\ \delta|\beta\end{cases}$, οπότε $\begin{cases}\delta|(\alpha-\kappa\beta)\\ \delta|\beta\end{cases}$. Άρα $\delta|(\alpha-\kappa\beta,\beta)$, δηλαδή $\delta|\delta'$ (1)

- $\begin{cases}\delta'|(\alpha-\kappa\beta)\\ \delta'|\beta\end{cases}$, οπότε $\begin{cases}\delta'|[(\alpha-\kappa\beta)+\kappa\beta]\\ \delta'|\beta\end{cases}$. Άρα $\begin{cases}\delta'|\alpha\\ \delta'|\beta\end{cases}$, οπότε $\delta'|(\alpha,\beta)$, δηλαδή $\delta'|\delta$. (2)

Από (1) και (2) έπεται ότι $\delta=\delta'$.

(ii) Λόγω της (i), για $\kappa=1$, ισχύει $(\alpha,\beta)=(\alpha-\beta,\beta)$.

(iii) Είναι: $(\alpha,\alpha+1)=(\alpha,\alpha+1-\alpha)=(\alpha,1)=1$.

2. Αν για τους ακεραίους α,β,γ ισχύει $\alpha|\gamma,\beta|\gamma$ και $(\alpha,\beta)=1$, τότε $\alpha\beta|\gamma$.

ΑΠΟΔΕΙΞΗ

Επειδή $(\alpha,\beta)=1$, υπάρχουν ακέραιοι κ,λ με $\kappa\alpha+\lambda\beta=1$. Επομένως,

$$\kappa\alpha\gamma+\lambda\beta\gamma=\gamma. \qquad (1)$$

Όμως, $\alpha|\gamma$ και $\beta|\gamma$, επομένως, $\gamma=\mu\alpha$ και $\gamma=\nu\beta$. Έτσι, η (1) γίνεται $\kappa\nu(\alpha\beta)+\lambda\mu(\alpha\beta)=\gamma$. Άρα $\alpha\beta|\gamma$.

3. (i) Αν $\kappa>0$, να αποδειχτεί ότι $(\kappa\alpha,\kappa\beta)=\kappa(\alpha,\beta)$.
(ii) Να βρεθεί ο Μ.Κ.Δ. των 63 και 84.

ΛΥΣΗ

(i) Έστω $(\alpha,\beta)=\delta$ και $(\kappa\alpha,\kappa\beta)=\delta'$. Αρκεί να δείξουμε ότι $\kappa\delta|\delta'$ και $\delta'|\kappa\delta$.
Επειδή $\delta|\alpha$ και $\delta|\beta$, έχουμε $\kappa\delta|\kappa\alpha$ και $\kappa\delta|\kappa\beta$. Άρα $\kappa\delta|\delta'$.
Αφού $\delta=(\alpha,\beta)$, υπάρχουν ακέραιοι μ και ν με $\mu\alpha+\nu\beta=\delta$ και επομένως, $\kappa\mu\alpha+\kappa\nu\beta=\kappa\delta$. Όμως $\delta'|\kappa\alpha$ και $\delta'|\kappa\beta$. Άρα $\delta'|\kappa\delta$.
(ii) Έχουμε $(63,84)=(3\cdot21,3\cdot28)$
$=3\cdot(21,28)=3\cdot(7\cdot3,7\cdot4)$
$=3\cdot7\cdot(3,4)$
$=3\cdot7\cdot1=\mathbf{21}$.

Ελάχιστο Κοινό Πολλαπλάσιο Ακεραίων

Ας θεωρήσουμε δύο ακεραίους α και β διαφορετικούς από το μηδέν. Ένας ακέραιος γ θα λέγεται **κοινό πολλαπλάσιο** των α και β, όταν είναι πολλαπλάσιο και του α και του β. Επειδή ο θετικός ακέραιος $|\alpha|\cdot|\beta|$ είναι κοινό πολλαπλάσιο των α και β, το σύνολο των θετικών πολλαπλάσιων των α και β είναι διάφορο του κενού συνόλου. Το ελάχιστο στοιχείο του συνόλου αυτού λέγεται ελάχιστο κοινό πολλαπλάσιο των α και β.

ΟΡΙΣΜΟΣ

Έστω δύο ακέραιοι α και β, διαφορετικοί από το μηδέν. Ορίζουμε ως **ελάχιστο κοινό πολλαπλάσιο** (Ε.Κ.Π.) των α και β, και το συμβολίζουμε με $\boldsymbol{[\alpha,\beta]}$, το μικρότερο από τα θετικά κοινά πολλαπλάσια των α και β.

Επομένως, το Ε.Κ.Π. δύο μη μηδενικών ακεραίων α και β είναι ο μοναδικός θετικός ακέραιος ε που έχει τις επόμενες δύο ιδιότητες:

(1) $\varepsilon = \text{πολ}\alpha$ και $\varepsilon = \text{πολ}\beta$

(2) $\varepsilon \le x$ για κάθε κοινό πολλαπλάσιο x των α και β.

Από τον ορισμό προκύπτει ότι

$$\boldsymbol{[\alpha,\beta]=[|\alpha|,|\beta|]}.$$

Έτσι, για παράδειγμα, για τους ακεραίους -4 και 6 έχουμε $[-4,6]=[4,6]=12$, αφού τα θετικά πολλαπλάσια του 4 είναι $4,8,12,16,20,24,28,...$, του 6 είναι τα $6,12,18,24,30,36,...$, τα θετικά κοινά τους πολλαπλάσια είναι $12,24,36,...$ και το μικρότερο θετικό κοινό πολλαπλάσιο είναι το 12.
Παρατηρούμε επίσης ότι για *θετικούς* ακεραίους α, β ισχύει:

- Αν $\beta|\alpha$, τότε $[\alpha,\beta]=\alpha$.
- $[\alpha,1]=\alpha$.

ΘΕΩΡΗΜΑ 5

Αν α, β είναι δύο *θετικοί* ακέραιοι, τότε

$$(\alpha,\beta)\cdot[\alpha,\beta]=\alpha\cdot\beta.$$

ΑΠΟΔΕΙΞΗ *

Αν $(\alpha, \beta)=\delta$, αρκεί να δείξουμε ότι $\frac{\alpha\beta}{\delta}=[\alpha,\beta]$, αρκεί δηλαδή να δείξουμε ότι

(i) $\frac{\alpha\beta}{\delta} = \text{πολ}\alpha$ και $\frac{\alpha\beta}{\delta} = \text{πολ}\beta$ και

(ii) $\frac{\alpha\beta}{\delta} \le x$ για κάθε θετικό κοινό πολλαπλάσιο x των α και β.

Επειδή $(\alpha,\beta)=\delta$, υπάρχουν θετικοί ακέραιοι μ και ν με $\alpha=\mu\delta$ και $\beta=\nu\delta$. Επομένως,

$$\frac{\alpha\beta}{\delta}=\frac{\alpha\delta\nu}{\delta}=\nu\alpha=\text{πολ}\alpha \qquad \text{και} \qquad \frac{\alpha\beta}{\delta}=\frac{\mu\delta\beta}{\delta}=\mu\beta=\text{πολ}\beta .$$

Αν x είναι ένα θετικό κοινό πολλαπλάσιο των α και β, τότε $x=\rho\alpha$ και $x=\sigma\beta$, όπου ρ και σ θετικοί ακέραιοι. Ξέρουμε επίσης ότι υπάρχουν ακέραιοι κ,λ με $\delta=\kappa\alpha+\lambda\beta$. Έτσι, αν θέσουμε $\frac{\alpha\beta}{\delta}=\tau$, τότε θα έχουμε

$$\frac{x}{\tau}=\frac{x\delta}{\alpha\beta}=\frac{x(\kappa\alpha+\lambda\beta)}{\alpha\beta}=\frac{x\kappa\alpha}{\alpha\beta}+\frac{x\lambda\beta}{\alpha\beta}=\frac{x\kappa}{\beta}+\frac{x\lambda}{\alpha}=\frac{\sigma\beta\kappa}{\beta}+\frac{\rho\alpha\lambda}{\alpha}=\sigma\kappa+\rho\lambda\in\mathbf{Z} .$$

Επομένως $\frac{\alpha\beta}{\delta}\Big|x$, οπότε $\frac{\alpha\beta}{\delta}\le x$. ■

Αν $\alpha,\ \beta\in\mathbf{Z}^*$, τότε από τις ισότητες $(\alpha,\beta)=(|\alpha|,|\beta|)$ και $[\alpha,\beta]=[|\alpha|,|\beta|]$, έχουμε

$$\boldsymbol{(\alpha,\beta)\cdot[\alpha,\beta]=|\alpha|\cdot|\beta|}$$

Από το παραπάνω θεώρημα προκύπτουν δύο σημαντικά πορίσματα:

- Αν οι ακέραιοι α και β είναι πρώτοι μεταξύ τους, τότε $[\alpha,\beta]=|\alpha|\cdot|\beta|$. Δηλαδή:

"Το Ε.Κ.Π. δύο πρώτων μεταξύ τους ακεραίων είναι το γινόμενο των απόλυτων τιμών τους".

Για παράδειγμα, $[8,-15]=8\cdot15=120$, αφού $(8,15)=1$.

- Το Ε.Κ.Π. δύο ακέραιων $\alpha,\ \beta$ διαιρεί κάθε άλλο κοινό πολλαπλάσιο x των α και β, δηλαδή είναι $x=\text{πολ}[\alpha,\beta]$. Άρα:

"Τα κοινά πολλαπλάσια δύο ακεραίων είναι τα πολλαπλάσια του Ε.Κ.Π.".

Για παράδειγμα, τα κοινά πολλαπλάσια των 4 και 6 είναι πολλαπλάσια του $[4,6]=12$, δηλαδή οι ακέραιοι $\pm12,\pm24,\pm36,\pm48,...$

Η έννοια του ελάχιστου κοινού πολλαπλάσιου γενικεύεται και για περισσότερους από δύο ακεραίους. Συγκεκριμένα, αν $\alpha_1,\alpha_2,\alpha_3,...,\alpha_\nu\in\mathbf{Z}^*$, τότε ορίζουμε ως ελάχιστο κοινό πολλαπλάσιο (Ε.Κ.Π.) των $\alpha_1,\alpha_2,\alpha_3,...,\alpha_\nu$, και το συμβολίζουμε με $[\alpha_1,\alpha_2,\alpha_3,...,\alpha_\nu]$, το μικρότερο από τα θετικά κοινά τους πολλαπλάσια. Αποδεικνύεται ότι:

"Το ελάχιστο κοινό πολλαπλάσιο τριών ή περισσότερων ακεραίων δε μεταβάλλεται, αν αντικαταστήσουμε δύο από αυτούς με το ελάχιστο κοινό τους πολλαπλάσιο".

Για παράδειγμα, $[4,6,16]=\big[[4,6],16\big]=[12,16]=48$.

ΕΦΑΡΜΟΓΗ

i) Να αποδειχτεί ότι $[\kappa\alpha,\kappa\beta]=\kappa[\alpha,\beta]$ για κάθε θετικό ακέραιο κ.

ii) Να βρεθεί το Ε.Κ.Π. των 120 και 150.

ΑΠΟΔΕΙΞΗ

(i) Έχουμε $[\kappa\alpha,\kappa\beta]=\dfrac{(\kappa\alpha)\cdot(\kappa\beta)}{(\kappa\alpha,\kappa\beta)}=\dfrac{\kappa^2}{\kappa}\cdot\dfrac{\alpha\beta}{(\alpha,\beta)}=\kappa\dfrac{\alpha\beta}{(\alpha,\beta)}=\kappa[\alpha,\beta]$

(ii) Έχουμε $[120,150]=[10\cdot12,10\cdot15]$

$=10\cdot[12,15]$

$=10\cdot[3\cdot4,3\cdot5]$

$=10\cdot3\cdot[4,5]$

$=30\cdot20=$**600** .

ΑΣΚΗΣΕΙΣ

Α΄ ΟΜΑΔΑΣ

1. Να βρείτε το Μ.Κ.Δ. των ακεραίων α,β και να τον εκφράσετε ως γραμμικό συνδυασμό των α και β σε καθεμιά από τις παρακάτω περιπτώσεις

(i) $\alpha=135$ και $\beta=56$, (ii) $\alpha=180$ και $\beta=84$

(iii) $\alpha=-180$ και $\beta=84$, (iv) $\alpha=-180$ και $\beta=-84$.

2. Να αποδείξετε ότι

(i) $(2\kappa+2,2\kappa)=2$, $\kappa\in\mathbf{Z}$ (ii) $(2\nu-1,2\nu+1)=1$, $\nu\in\mathbf{N}^*$

(iii) $[2\nu-1,2\nu+1]=(2\nu-1)(2\nu+1)$, $\nu\in\mathbf{N}^*$ (iv) $(\nu+2,2)\mid\nu$, $\nu\in\mathbf{N}^*$

(v) $[\nu,\nu+1]=\nu(\nu+1)$, $\nu\in\mathbf{N}^*$.

3. Να αποδείξετε ότι $(\alpha,\beta)\le(\alpha+\beta,\alpha-\beta)$.

4. Έστω $\alpha,\beta,x,y\in\mathbf{Z}$, με $\alpha x-\beta y=1$. Να αποδείξετε ότι $(\alpha+\beta,x+y)=1$.

5. Να αποδείξετε ότι
(i) $(2\alpha-3\beta,4\alpha-5\beta)|\beta$ (ii) $(2\alpha+3,\ 4\alpha+5)=1$ (iii) $(5\alpha+2,\ 7\alpha+3)=1$.

6. Να αποδείξετε ότι για κάθε $\kappa\in\mathbf{Z}$ ισχύει:
(i) $\left(2\kappa+1,\ \frac{\kappa(\kappa+1)}{2}\right)=1$, (ii) $(4\kappa^2+3\kappa-5,\ 2\kappa^2+\kappa-2)=1$.

7. Να αποδείξετε ότι $(\alpha,\ \beta,\ \alpha+\beta)=(\alpha,\beta)$.

8. Να βρείτε το θετικό ακέραιο α για τον οποίο ισχύει
(i) $(\alpha,\alpha+\nu)=1$, για κάθε $\nu\in\mathbf{N}^*$
(ii) $(\nu,\alpha+\nu)=1$, για κάθε $\nu\in\mathbf{N}^*$.

9. Αν $(\alpha,\beta)=1$ και $\gamma|(\alpha+\beta)$, να αποδείξετε ότι $(\alpha,\gamma)=(\beta,\gamma)=1$.

Β΄ ΟΜΑΔΑΣ

1. Αν $(\alpha,\beta)=1$, να αποδείξετε ότι:
(i) $(\alpha+\beta,\ \alpha-\beta)=1$ ή 2 (ii) $(2\alpha+\beta,\ \alpha+2\beta)=1$ ή 3.

2. Αν $(\alpha,4)=2$ και $(\beta,4)=2$, να αποδείξετε ότι $(\alpha+\beta,\ 4)=4$.

3. Να εξετάσετε αν υπάρχουν θετικοί ακέραιοι ν, για τους οποίους το κλάσμα $\frac{2\nu+3}{5\nu+7}$ απλοποιείται.

4. Έστω $\alpha,\beta\in\mathbf{N}^*$. Να αποδείξετε ότι: $(\alpha,\beta)=[\alpha,\beta]\Leftrightarrow\alpha=\beta$.

5. Ένας μαθητής στην προσπάθειά του να βρει το Μ.Κ.Δ. τριών ακεραίων α,β,γ βρήκε:
$(\alpha,\beta)=9$, $(\beta,\gamma)=30$ και $(\gamma,\alpha)=12$.
Μπορείτε να απαντήσετε αν έκανε ή όχι λάθος;

6. Έστω $\alpha,\beta\in\mathbf{Z}$ με $(\alpha,\beta)=\delta$. Να αποδείξετε ότι οι αριθμοί $\kappa,\lambda\in\mathbf{Z}$ για τους οποίους ισχύει $\delta=\kappa\alpha+\lambda\beta$ είναι πρώτοι μεταξύ τους.

7. Έστω $\alpha,\beta,\kappa\in\mathbf{N}^*$ με $(\alpha,\kappa)=1$. Να αποδείξετε ότι
(i) $(\alpha,\kappa\beta)=(\alpha,\beta)$ (ii) $[\alpha,\kappa\beta]=\kappa[\alpha,\beta]$.

8. Έστω $\alpha,\beta,\gamma,\delta\in\mathbf{N}^*$. Να αποδείξετε ότι $[\alpha\gamma,\beta\gamma,\alpha\delta,\beta\delta]=[\alpha,\beta]\cdot[\gamma,\delta]$.

4.5 ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

Εισαγωγή

Δύο από τα σημαντικότερα αποτελέσματα σχετικά με τους πρώτους αριθμούς ήταν γνωστά ήδη από την αρχαιότητα. Το γεγονός ότι κάθε ακέραιος αναλύεται με μοναδικό τρόπο ως γινόμενο πρώτων εμφανίζεται στα "Στοιχεία" του Ευκλείδη στην εξής μορφή (βιβλίο IX, πρόταση 14):

"Εάν ελάχιστος αριθμός υπό πρώτων αριθμών μετρήται, υπ' ουδενός άλλου πρώτου αριθμού μετρηθήσεται παρέξ των εξ αρχής μετρούντων".

Στα "Στοιχεία" επίσης, το γεγονός ότι υπάρχουν άπειροι πρώτοι αριθμοί εμφανίζεται ως εξής (βιβλίο IX, πρόταση 20):

"Οι πρώτοι αριθμοί πλείους εισί παντός του προτεθέντος πλήθους πρώτων αριθμών".

Το αποτέλεσμα αυτό και η απόδειξή του από τον Ευκλείδη θεωρούνται ένα από τα αριστουργήματα της θεωρητικής μαθηματικής σκέψης. Ο G. Hardy (1877-1947) έγραψε ότι "… είναι τόσο σύγχρονο και σημαντικό όπως και όταν ανεκαλύφθη-εδώ και 2000 χρόνια παρέμεινε ανέπαφο".

Ο μεγαλύτερος πρώτος αριθμός που έχει εντοπιστεί μέχρι σήμερα είναι ο $2^{2.976.221}-1$, ένας "γίγαντας" με 895.932 ψηφία. Πρόκειται για τον 36ο από τους πρώτους αριθμούς της μορφής $2^{\nu}-1$ που γνωρίζουμε και ο οποίος οδήγησε στην ανακάλυψη του 36ου τέλειου αριθμού (βλπ. προηγούμενο ιστορικό σημείωμα). Οι τεράστιοι αυτοί αριθμοί εντοπίστηκαν με τη βοήθεια κριτηρίων αναγνώρισης πρώτων, που απαιτούν πολύωρη χρήση ηλεκτρονικών υπολογιστών.

Άλλοι πρώτοι αριθμοί με ιδιαίτερο ενδιαφέρον είναι αυτοί της μορφής $p=2^{\nu}+1$, όπου $\nu=2^{\kappa}$, από τους οποίους όμως γνωρίζουμε μόνο 5, αυτούς που προκύπτουν για $\kappa=0,1,2,3,4$ και είναι αντίστοιχα οι $3,5,17,257,65537$ (όσοι από τους υπόλοιπους έχουν ελεγχθεί αποδείχτηκαν σύνθετοι). Ο C.F. Gauss σε πολύ νεαρή ηλικία έδειξε ότι ένα κανονικό πολύγωνο κατασκευάζεται με κανόνα και διαβήτη, μόνο αν το πλήθος των πλευρών του είναι πρώτος αριθμός αυτής της μορφής ή γινόμενο πρώτων αυτής της μορφής πολλαπλασιασμένο επί μια δύναμη του 2 ή απλώς μια δύναμη του 2.

Το σημαντικότερο όμως ζήτημα σχετικά με τους πρώτους αριθμούς αφορά την κατανομή τους μέσα στην ακολουθία των φυσικών. Η κατανομή αυτή είναι πολύ ακανόνιστη, γιατί από τη μια μεριά υπάρχουν εκατομμύρια ζεύγη των λεγόμενων δίδυμων πρώτων, όπως ,για παράδειγμα, οι $(29, 31)$, $(1451, 1453)$, $(299477, 299479)$, ενώ από την άλλη υπάρχουν τεράστια κενά χωρίς κανέναν πρώτο. Μια σχετική τάξη στο χάος βάζει το "Θεώρημα των πρώτων αριθμών", σύμφωνα με το οποίο το πλήθος των πρώτων αριθμών που είναι μικρότεροι ή

ίσοι από τον φυσικό ν δίνεται κατά προσέγγιση (καθώς το ν γίνεται πολύ μεγάλο) από τον τύπο $\nu/\ln\nu$. Αυτό το διαπίστωσαν εμπειρικά, μελετώντας πίνακες πρώτων αριθμών, οι A.M. Legendre και C.F. Gauss στα τέλη του 18ου αιώνα, ενώ η πρώτη αυστηρή απόδειξη δόθηκε 100 χρόνια αργότερα.

Έννοια Πρώτου Αριθμού

Παρατηρήσαμε προηγουμένως ότι κάθε ακέραιος $\alpha \neq 0,\pm 1$ διαιρείται με τους ακέραιους ± 1 και $\pm\alpha$. Αν αυτοί είναι και οι μόνοι διαιρέτες του α, τότε αυτός λέγεται πρώτος αριθμός. Δηλαδή:

ΟΡΙΣΜΟΣ

Κάθε ακέραιος $p \neq 0,\pm 1$ λέγεται **πρώτος αριθμός** ή απλώς **πρώτος**, αν οι μόνοι θετικοί διαιρέτες του είναι οι 1 και $|p|$.

Για παράδειγμα, οι ακέραιοι 2 και -7 είναι πρώτοι, ενώ ο $8=2\cdot 4$ και ο $-39=3\cdot(-13)$ δεν είναι πρώτοι.

Ένας ακέραιος $\alpha \neq \pm 1$ που δεν είναι πρώτος λέγεται **σύνθετος**. Ένας σύνθετος αριθμός α μπορεί να γραφεί ως γινόμενο $\beta\cdot\gamma$ με $\beta \neq \pm 1$ και $\gamma \neq \pm 1$.

Οι αριθμοί 1 και -1 δε χαρακτηρίζονται ούτε ως πρώτοι ούτε ως σύνθετοι.

Κάθε πρώτος που διαιρεί ένα δοθέντα ακέραιο λέγεται **πρώτος διαιρέτης** του ακεραίου αυτού. Είναι φανερό ότι ο $-\alpha$ είναι πρώτος, αν και μόνο αν ο α είναι πρώτος. Γι' αυτό στη συνέχεια θα περιοριστούμε **μόνο** σε θετικούς πρώτους. Ανάμεσα στους δέκα αριθμούς $1,2,3,\ldots,10$ οι $2,3,5$ και 7 είναι πρώτοι, ενώ οι $4,6,8,$ και 10 είναι σύνθετοι. Ο αριθμός 2 είναι ο μοναδικός άρτιος που είναι πρώτος, όλοι οι άλλοι πρώτοι είναι περιττοί.

Ένα εύλογο ερώτημα είναι το εξής:

"Αν δοθεί ένας θετικός ακέραιος α, πώς μπορούμε να αποφανθούμε αν είναι πρώτος ή σύνθετος και, στην περίπτωση που είναι σύνθετος, πώς μπορούμε πρακτικά να βρούμε ένα διαιρέτη διαφορετικό από τους 1 και α";

Η προφανής απάντηση είναι να κάνουμε διαδοχικές διαιρέσεις με τους ακεραίους που είναι μικρότεροι του α. Αν κανένας από αυτούς δε διαιρεί τον α, τότε ο α είναι πρώτος. Αν και η μέθοδος αυτή είναι πολύ απλή στην περιγραφή της, δεν μπορεί να θεωρηθεί πρακτική, γιατί έχει απαγορευτικό κόστος σε χρόνο και εργασία, ιδιαίτερα για μεγάλους αριθμούς.

Υπάρχουν ιδιότητες των σύνθετων ακεραίων που αναφέρονται στα επόμενα θεωρήματα και μας επιτρέπουν να περιορίσουμε σημαντικά τους αναγκαίους υπολογισμούς.

ΘΕΩΡΗΜΑ 6

Κάθε θετικός ακέραιος μεγαλύτερος του 1 έχει έναν τουλάχιστον πρώτο διαιρέτη.

ΑΠΟΔΕΙΞΗ

Έστω ο θετικός ακέραιος $\alpha>1$ και p ο μικρότερος από τους θετικούς διαιρέτες του με $p>1$. Θα αποδείξουμε ότι ο p είναι πρώτος αριθμός. Αν ο p ήταν σύνθετος, θα είχε ένα θετικό διαιρέτη, έστω β με $1<\beta<p$. Αφού όμως $\beta|p$ και $p|\alpha$, τότε θα ισχύει $\beta|\alpha$ (θεώρημα 2). Βρήκαμε έτσι ένα θετικό διαιρέτη β του α που είναι μικρότερος του p. Αυτό όμως είναι άτοπο, αφού ο p θεωρήθηκε ως ο ελάχιστος διαιρέτης του α. Έτσι ο μικρότερος από τους θετικούς διαιρέτες ενός ακεραίου είναι πρώτος αριθμός. ■

ΠΟΡΙΣΜΑ 4

Αν α είναι ένας σύνθετος ακέραιος με $\alpha>1$, τότε υπάρχει ένας τουλάχιστον πρώτος αριθμός p, τέτοιος, ώστε $p|\alpha$ και $p\le\sqrt{\alpha}$.

ΑΠΟΔΕΙΞΗ

Επειδή ο α είναι σύνθετος, γράφεται στη μορφή

$$\alpha=\beta\cdot\gamma, \qquad \text{με } 1<\beta<\alpha \quad \text{και} \quad 1<\gamma<\alpha.$$

Υποθέτουμε ότι $\beta\le\gamma$, οπότε $\beta^2\le\beta\gamma=\alpha$ και επομένως $\beta\le\sqrt{\alpha}$. Αφού $\beta>1$, ο β έχει έναν τουλάχιστον πρώτο διαιρέτη p και επομένως $p\le\beta\le\sqrt{\alpha}$. Επειδή $p|\beta$ και $\beta|\alpha$, θα ισχύει $p|\alpha$. Επομένως, ο πρώτος p διαιρεί τον α και είναι $p\le\sqrt{\alpha}$. ■

Το παραπάνω συμπέρασμα έχει μεγάλη πρακτική σημασία όταν εξετάζουμε αν ένας ακέραιος $\alpha>1$ είναι πρώτος ή όχι, αφού περιορίζει τις δοκιμές στους πρώτους αριθμούς που είναι μικρότεροι ή ίσοι της $\sqrt{\alpha}$.

Έστω, για παράδειγμα, ο ακέραιος $\alpha=271$. Επειδή $16<\sqrt{271}<17$, χρειάζεται μόνο να εξετάσουμε αν οι πρώτοι που δεν υπερβαίνουν τον 16 είναι διαιρέτες του 271. Οι πρώτοι αυτοί είναι οι 2,3,5,7,11 και 13 και κανένας τους δε διαιρεί τον 271. Άρα, ο 271 είναι πρώτος.

Το Κόσκινο του Ερατοσθένη

Μια έξυπνη τεχνική για τον προσδιορισμό των πρώτων που δεν υπερβαίνουν ένα θετικό ακέραιο $\nu>1$ στηρίζεται στο προηγούμενο θεώρημα και την οφείλουμε στον Αρχαίο Έλληνα μαθηματικό Ερατοσθένη (περίπου 250 π.Χ.). Η τεχνική λέγεται **κόσκινο του Ερατοσθένη** και είναι η εξής:
Γράφουμε σε έναν πίνακα με αύξουσα σειρά τους ακεραίους από 2 μέχρι ν. Αφήνουμε τον πρώτο 2 και διαγράφουμε όλα τα πολλαπλάσιά του. Ο επόμενος πρώτος στον πίνακα μετά τον 2 είναι ο 3. Αφήνουμε τον 3 και διαγράφουμε όλα τα πολλαπλάσιά του κτλ. Συνεχίζουμε την ίδια διαδικασία μέχρι τον πρώτο p με $p \le \sqrt{\nu}$. Οι ακέραιοι που απομένουν, δηλαδή όσοι δεν "έπεσαν" από το "κόσκινο", είναι οι πρώτοι μεταξύ 2 και ν. Όλοι οι άλλοι "έπεσαν", διότι, ως σύνθετοι, είχαν διαιρέτη κάποιον πρώτο μικρότερο ή ίσο της $\sqrt{\nu}$ και ως πολλαπλάσια του διαγράφηκαν.

Στον παρακάτω πίνακα έχουν προσδιοριστεί οι πρώτοι μεταξύ 1 και 100. Έχουν διαγραφεί τα πολλαπλάσια των πρώτων $2,3,5$ και 7, αφού ο επόμενος πρώτος είναι ο αριθμός 11 και ισχύει $11>\sqrt{100}$.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Στο σημείο αυτό πιθανόν να αναρωτηθεί κάποιος: Τελειώνουν κάπου οι πρώτοι; Υπάρχει δηλαδή μέγιστος πρώτος ή οι πρώτοι συνεχίζονται “επ’άπειρον”;

ΘΕΩΡΗΜΑ 7 (του Ευκλείδη)

Υπάρχουν *άπειροι* θετικοί πρώτοι αριθμοί.

ΑΠΟΔΕΙΞΗ

Έστω ότι υπάρχει πεπερασμένο πλήθος πρώτων αριθμών $p_1, p_2, ..., p_\nu$. Θα αποδείξουμε ότι αυτό οδηγεί σε άτοπο. Σχηματίζουμε τον αριθμό $\boldsymbol{A = p_1 p_2 \dots p_\nu + 1}$. Ο αριθμός όμως αυτός, επειδή είναι μεγαλύτερος του 1, θα έχει έναν τουλάχιστον πρώτο διαιρέτη, έστω τον p_i με $1 \le i \le \nu$. Αλλά αν ο p_i διαιρεί τον A, επειδή διαιρεί και τον $p_1 p_2 \dots p_\nu$, θα πρέπει να διαιρεί και τον 1. Αυτό όμως είναι άτοπο, γιατί $p_i > 1$. ■

Θεμελιώδες Θεώρημα Αριθμητικής

Οι πρώτοι αριθμοί έχουν μεγάλη σπουδαιότητα για τη Θεωρία των Αριθμών, αφού, όπως θα αποδείξουμε στο *Θεμελιώδες Θεώρημα της Αριθμητικής*, κάθε φυσικός αναλύεται με μοναδικό τρόπο σε γινόμενο πρώτων παραγόντων. Με άλλα λόγια οι πρώτοι αριθμοί αποτελούν τα δομικά υλικά με τα οποία, μέσω του πολλαπλασιασμού κατασκευάζουμε τους άλλους φυσικούς αριθμούς, όπως για παράδειγμα στη Χημεία με κατάλληλα άτομα σχηματίζουμε τα μόρια των διάφορων ουσιών.
Η απόδειξη του σημαντικού αυτού θεωρήματος στηρίζεται στον ακόλουθο αληθή ισχυρισμό.

ΘΕΩΡΗΜΑ 8

Αν ένας πρώτος p διαιρεί το γινόμενο $\alpha\beta$ δύο ακέραιων, τότε διαιρεί έναν, τουλάχιστον, από τους ακεραίους αυτούς.

ΑΠΟΔΕΙΞΗ

Έστω ότι $p|\alpha$. Επειδή ο αριθμός p είναι πρώτος, οι μοναδικοί διαιρέτες του είναι οι 1 και p. Επομένως, ο Μ.Κ.Δ. των α και p είναι $(p,\alpha)=1$, δηλαδή ο p είναι πρώτος προς τον a. Αφού λοιπόν $p|\alpha\beta$ και $(p,\alpha)=1$, σύμφωνα με το Πόρισμα 3, $p|\beta$. ■

Το θεώρημα ισχύει και για γινόμενο περισσότερων ακεραίων. Δηλαδή:
"Αν p πρώτος και $p|\alpha_1\alpha_2\alpha_3 ... \alpha_\nu$, τότε ο p διαιρεί έναν, τουλάχιστον, από τους παράγοντες του γινομένου".

ΘΕΩΡΗΜΑ 9

Κάθε θετικός ακέραιος $\alpha > 1$ αναλύεται κατά μοναδικό τρόπο ως γινόμενο πρώτων παραγόντων (αν παραβλέψουμε τη σειρά των παραγόντων).

ΑΠΟΔΕΙΞΗ *

- Αν ο α είναι πρώτος, τότε προφανώς το θεώρημα ισχύει.

Αν ο α είναι σύνθετος, τότε, σύμφωνα με το θεώρημα 6, θα ισχύει $\alpha = p_1 \cdot \beta_1$, όπου p_1 πρώτος και β_1 ακέραιος με $\alpha > \beta_1 > 1$.

Αν ο β_1 είναι πρώτος, τότε ο α είναι γινόμενο πρώτων παραγόντων και το θεώρημα αληθεύει.

Αν ο β_1 είναι σύνθετος, τότε θα έχουμε $\beta_1 = p_2 \cdot \beta_2$, με p_2 πρώτο και $\alpha > \beta_2 > 1$.

Αν ο β_2 είναι πρώτος, τότε $\alpha = p_1 \cdot p_2 \cdot \beta_2$ και ο α είναι γινόμενο πρώτων παραγόντων.

Αν ο β_2 είναι σύνθετος, τότε η παραπάνω διαδικασία μπορεί να συνεχιστεί και οδηγεί σε μια σχέση $\alpha = p_1 \cdot p_2 \cdot p_3 \cdot \beta_3$, με p_3 πρώτο και $\alpha > \beta_1 > \beta_2 > \beta_3 > 1$.

Αποδεικνύεται ότι αν συνεχίσουμε τη διαδικασία αυτή, ύστερα από ένα πεπερασμένο πλήθος βημάτων θα βρούμε τελικά έναν πρώτο p_κ, τέτοιο, ώστε

$$\alpha = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_\kappa .$$

- Ας υποθέσουμε ότι ο α αναλύεται και με άλλο τρόπο σε γινόμενο πρώτων παραγόντων, ότι δηλαδή υπάρχουν και οι πρώτοι $q_1, q_2, q_3, \ldots, q_\lambda$, τέτοιοι, ώστε

$$\alpha = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_\kappa = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_\lambda \qquad (1)$$

και έστω ότι $\kappa \leq \lambda$. Ο πρώτος p_1 είναι διαιρέτης του α άρα και του γινομένου $q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_\lambda$. Επομένως, σύμφωνα με το θεώρημα 8, ο p_1 θα είναι διαιρέτης ενός τουλάχιστον από τους παράγοντες $q_1, q_2, q_3, \ldots, q_\lambda$, έστω $p_1 | q_\mu$, όπου $1 < \mu < \lambda$.

Ο q_μ όμως είναι πρώτος και έχει ως διαιρέτες μόνο το 1 και τον εαυτό του. Άρα, επειδή $p_1 \neq 1$, θα είναι $p_1 = q_\mu$. Ύστερα από τη διαγραφή των δυο αυτών ίσων παραγόντων, με ανάλογο συλλογισμό συμπεραίνουμε ότι ο p_2 πρέπει να είναι ίσος με έναν, τουλάχιστον από τους υπόλοιπους παράγοντες του δεύτερου μέλους της (1) π.χ. τον q_τ. Αφού διαγράψουμε τους p_2 και q_τ, συνεχίζουμε ομοίως με τους $p_3, \ldots, p_\kappa$. Στο τέλος της διαδικασίας όλοι οι παράγοντες $p_1, p_2, p_3, \ldots, p_\kappa$ θα έχουν διαγραφεί, αφήνοντας μόνο τον αριθμό 1 στο πρώτο μέλος της ισότητας (1). Κανένας όμως και από τους παράγοντες $q_1, q_2, q_3, \ldots, q_\lambda$ δε θα έχει απομείνει και στο δεύτερο μέλος της (1), αφού όλοι αυτοί οι παράγοντες είναι μεγαλύτεροι από το 1. Έτσι, οι παράγοντες $p_1, p_2, p_3, \ldots, p_\kappa$ του πρώτου μέλους σχηματίζουν ζεύγη ίσων αριθμών με τους παράγοντες του δεύτερου μέλους. Αυτό αποδεικνύει ότι, με εξαίρεση ίσως τη σειρά των παραγόντων, οι δύο αναλύσεις του αριθμού είναι ταυτόσημες. ■

Βέβαια, μερικοί από τους πρώτους παράγοντες που εμφανίζονται στην ανάλυση ενός θετικού ακεραίου μπορεί να επαναλαμβάνονται όπως στην περίπτωση του 360 για τον οποίο έχουμε $360=2\cdot2\cdot2\cdot3\cdot3\cdot5$. Γράφοντας τα γινόμενα των ίδιων παραγόντων με μορφή δυνάμεων, μπορούμε να επαναδιατυπώσουμε το θεώρημα ως εξής:

Κάθε θετικός ακέραιος $\alpha>1$ μπορεί να γραφεί κατά μοναδικό τρόπο στη μορφή: $\alpha = p_1^{\alpha_1}\cdot p_2^{\alpha_2}...p_\kappa^{\alpha_\kappa}$,
όπου οι $p_1,p_2,...,p_\kappa$ είναι θετικοί πρώτοι με $p_1 < p_2 <...< p_\kappa$ και $\alpha_1,\alpha_2,...,\alpha_\kappa$ θετικοί ακέραιοι.

Η μορφή $\alpha = p_1^{\alpha_1}\cdot p_2^{\alpha_2}...p_\kappa^{\alpha_\kappa}$ λέγεται και **κανονική μορφή** του α.

Μ.Κ.Δ. και Ε.Κ.Π. Αριθμών σε Κανονική Μορφή

Όταν είναι γνωστή η ανάλυση ενός φυσικού αριθμού α σε πρώτους παράγοντες, εύκολα μπορούμε να επισημάνουμε τους διαιρέτες του.
Έστω $\alpha = p_1^{\alpha_1}\cdot p_2^{a_2}...p_\kappa^{\alpha_\kappa}$ η κανονική μορφή του α και d ένας θετικός διαιρέτης του. Αν p είναι ένας πρώτος που εμφανίζεται στην κανονική μορφή του d, τότε $p|\alpha$ και επομένως, πρέπει $p=p_i$ με $1\le i\le\kappa$. Επίσης ο p_i δεν μπορεί να εμφανίζεται στον αριθμό d περισσότερο από α_i φορές. Παρατηρούμε δηλαδή ότι ένας διαιρέτης d του α έχει στην κανονική του μορφή παράγοντες μόνο από τους $p_1,p_2,...,p_\kappa$ και με εκθέτες ίσους ή μικρότερους των $\alpha_1,\alpha_2,...,\alpha_\kappa$ αντιστοίχως. Για παράδειγμα, επειδή $12=2^3\cdot3^1$, οι διαιρέτες του 12 είναι οι $2^0\cdot3^0=1$, $2^1\cdot3^0=2$, $2^2\cdot3^0=4$, $2^0\cdot3^1=3$, $2^1\cdot3^1=6$ και $2^2\cdot3^1=12$.
Με βάση την παρατήρηση αυτή μπορούμε εύκολα να βρούμε Μ.Κ.Δ. και το Ε.Κ.Π. αριθμών που έχουν αναλυθεί σε πρώτους παράγοντες. Συγκεκριμένα:

- Ο Μ.Κ.Δ. θετικών ακεραίων που είναι γραμμένοι σε κανονική μορφή είναι ίσος με το γινόμενο των κοινών τους παραγόντων και με τον κάθε παράγοντα υψωμένο στο μικρότερο εμφανιζόμενο εκθέτη.
- Το Ε.Κ.Π. θετικών ακεραίων που είναι γραμμένοι σε κανονική μορφή είναι ίσο με το γινόμενο των κοινών και μη κοινών τους παραγόντων και με τον κάθε παράγοντα υψωμένο στο μεγαλύτερο εμφανιζόμενο εκθέτη.

Για παράδειγμα, επειδή $2520=2^3\cdot3^2\cdot5\cdot7$ και $756=2^2\cdot3^3\cdot7$, έχουμε $(2520,756)=2^2\cdot3^2\cdot7=\mathbf{252}$ και $[2520,756]=2^3\cdot3^3\cdot5\cdot7=\mathbf{7560}$.

ΕΦΑΡΜΟΓΕΣ

1. Να αποδειχτεί ότι αν ο αριθμός $2^\nu-1$, $\nu\in\mathbf{N}^*$ είναι πρώτος, τότε και ο ν είναι πρώτος.

ΑΠΟΔΕΙΞΗ

Αν ο ν δεν είναι πρώτος, τότε $\nu=\alpha\beta$ με α,β θετικούς ακέραιους και $\alpha,\beta>1$, οπότε έχουμε $2^\nu-1=2^{\alpha\beta}-1=(2^\alpha)^\beta-1$. Ο αριθμός αυτός, όμως, έχει ως παράγοντα τον $2^\alpha-1$, για τον οποίο ισχύει $\mathbf{1<2^\alpha-1<2^\nu-1}$. Επομένως, ο $2^\nu-1$ είναι σύνθετος που είναι άτοπο.

2. Αν ο φυσικός αριθμός ν δεν είναι τετράγωνο φυσικού, να αποδειχτεί ότι ο αριθμός $\sqrt{\nu}$ είναι άρρητος.

ΑΠΟΔΕΙΞΗ

Έστω ότι ο αριθμός $\sqrt{\nu}$ είναι ρητός. Τότε $\sqrt{\nu}=\frac{\alpha}{\beta}$, όπου α και β θετικοί ακέραιοι. Οι ακέραιοι α και β μπορούν να θεωρηθούν πρώτοι μεταξύ τους, γιατί αν δε συμβαίνει αυτό, τους διαιρούμε με το Μ.Κ.Δ. τους, οπότε μετατρέπονται σε πρώτους μεταξύ τους. Από την ισότητα $\sqrt{\nu}=\frac{\alpha}{\beta}$ έχουμε $\alpha^2=\nu\beta^2$. Επειδή ο ν δεν είναι τετράγωνο φυσικού θα είναι $\beta>1$. Επομένως, ο ακέραιος β θα έχει έναν πρώτο διαιρέτη p, οπότε θα ισχύει $p|\alpha^2$, δηλαδή $p|\alpha\cdot\alpha$ και άρα $p|\alpha$ (Θεώρημα 10). Επομένως, $p|\alpha$ και $p|\beta$, που είναι άτοπο, αφού οι α και β είναι πρώτοι μεταξύ τους.

ΑΣΚΗΣΕΙΣ

Α΄ Ομάδας

1. Ποιοι από τους παρακάτω αριθμούς είναι πρώτοι;

101, 103, 107, 111, 113, 121.

2. Να βρείτε το μικρότερο φυσικό αριθμό α για τον οποίο οι αριθμοί:
(i) $\alpha, \alpha+1, \alpha+2$ είναι όλοι σύνθετοι
(ii) $\alpha, \alpha+1, \alpha+2, \alpha+3$ είναι όλοι σύνθετοι

3. Να βρείτε τους $\alpha, \beta \in \mathbf{N}^*$ και τον πρώτο $p>3$ σε καθεμιά από τις παρακάτω περιπτώσεις:
(i) $(\alpha-\beta)(\alpha+\beta)=3$ (ii) $\alpha^2-4=p$ (iii) $(\alpha^2-1)p=15$

4. Να αποδείξετε ότι ο μοναδικός θετικός πρώτος p για τον οποίο ισχύει $3p+1=\nu^2$, όπου $\nu \in \mathbf{N}^*$, είναι ο $p=5$.

5. Να αποδείξετε ότι ο μοναδικός θετικός πρώτος p που μπορεί να πάρει τη μορφή $p=\nu^3-1$, $\nu \in \mathbf{N}^*$ είναι ο $p=7$, ενώ τη μορφή $p=\nu^3+1$, $\nu \in \mathbf{N}^*$, είναι ο $p=2$.

6. Αν α, β είναι δύο περιττοί θετικοί ακέραιοι μεγαλύτεροι του 1, να αποδείξετε ότι ο ακέραιος $\alpha^2+\beta^2$ είναι σύνθετος.

7. Έστω α, ν θετικοί ακέραιοι και p θετικός πρώτος. Αν $p|\alpha^\nu$, να αποδείξετε ότι $p^\nu|\alpha^\nu$.

8. Έστω $\alpha, \beta, \mu, \nu \in \mathbf{N}^*$ με $(\alpha, \beta)=1$. Να αποδείξετε ότι $(\alpha^\mu, \beta^\nu)=1$.

9. Να γράψετε στην κανονική τους μορφή τους φυσικούς αριθμούς 490, 1125, 2728 και να βρείτε το Μ.Κ.Δ. και το Ε.Κ.Π. αυτών.

10. Έστω $\alpha=p_1^{\alpha_1}p_2^{\alpha_2}...p_\kappa^{\alpha_\kappa}$ η κανονική μορφή ενός θετικού ακεραίου α. Να αποδείξετε ότι ο α είναι τετράγωνο ενός θετικού ακεραίου, αν και μόνο αν οι εκθέτες $\alpha_1, \alpha_2, ..., \alpha_\kappa$ είναι όλοι άρτιοι.

Β΄ ΟΜΑΔΑΣ

1. Αν $(\alpha, \beta)=1$, να αποδείξετε ότι
(i) $(\alpha+\beta, \alpha\beta)=1$, (ii) $(\alpha^2+\beta^2, \alpha\beta)=1$.

2. Να αποδείξετε την ισοδυναμία:
$$(\alpha, \beta\gamma)=1 \Leftrightarrow (\alpha, \beta)=(\alpha, \gamma)=1.$$

3. Έστω $\alpha, \beta \in \mathbf{N}^*$ και p θετικός πρώτος. Αν $(\alpha, p^2)=p$ και $(\beta, p^3)=p^2$, να βρείτε τον $(\alpha\beta, p^4)$ και τον $(\alpha+\beta, p^4)$.

4. Να αποδείξετε ότι οι ακέραιοι της μορφής ν^4+4, όπου ν θετικός ακέραιος μεγαλύτερος του 1, και οι ακέραιοι της μορφής $8^\nu+1$, όπου ν θετικός ακέραιος, είναι σύνθετοι αριθμοί.

5. Αν $\alpha,\beta\in\mathbf{N}^*$ με $\frac{\alpha}{\beta}=\frac{43}{34}$, να αποδείξετε ότι ο αριθμός $\alpha+\beta$ είναι σύνθετος.

6. Να αποδείξετε ότι ο μοναδικός θετικός πρώτος p για τον οποίον οι αριθμοί $p, p+2$ και $p+4$ είναι και οι τρεις πρώτοι είναι ο $p=3$.

7. Να λύσετε στο **N** τις εξισώσεις
(i) $x^3+x^2+x-3=0$ (ii) $x^2+x+p=112$, όπου p θετικός πρώτος.

8. Έστω $\alpha,\beta\in\mathbf{N}^*$. Αν $\beta^2|\alpha^2$, να αποδείξετε ότι $\beta|\alpha$.

4.6 Η ΓΡΑΜΜΙΚΗ ΔΙΟΦΑΝΤΙΚΗ ΕΞΙΣΩΣΗ

Εισαγωγή

Ένα από τα αρχαιότερα προβλήματα της Θεωρίας Αριθμών είναι η αναζήτηση των ακέραιων αριθμών που ικανοποιούν κάποιες δεδομένες σχέσεις. Με σύγχρονη ορολογία θα διατυπώσουμε το ίδιο πρόβλημα ως επίλυση, στο **Z**, πολυωνυμικών εξισώσεων με έναν ή περισσότερους αγνώστους και με ακέραιους συντελεστές. Ο κλάδος που ασχολείται με αυτό το ζήτημα ονομάζεται Διοφαντική Ανάλυση προς τιμήν του Διόφαντου (250 περίπου μ.Χ.), που ασχολήθηκε συστηματικά με τέτοιου είδους προβλήματα στο έργο του "Αριθμητικά".
Η αναζήτηση Πυθαγόρειων τριάδων (δηλαδή ακέραιων λύσεων της εξίσωσης $x^2+y^2=z^2$) συγκαταλέγεται ανάμεσα στα κλασικά προβλήματα της Διοφαντικής Ανάλυσης. Υπάρχουν ενδείξεις ότι η λύση αυτού του προβλήματος (που δίνεται σήμερα από τους τύπους $x=\mu^2-\nu^2$, $y=2\mu\nu$ $z=\mu^2+\nu^2$) ήταν γνωστή στους Βαβυλώνιους, αλλά η πλήρης θεωρητική διαπραγμάτευση του ζητήματος έγινε από τους Αρχαίους Έλληνες μαθηματικούς. Ο Ευκλείδης διατυπώνει το πρόβλημα στη μορφή

"Ευρείν δύο τετραγώνους αριθμούς, ώστε και το συγκείμενον εξ αυτών είναι τετράγωνον"

και δίνει τη γενική λύση στη γεωμετρική γλώσσα των "Στοιχείων" (Βιβλίο Χ, Λήμμα 1, Πρότ. 28).
Ο Διόφαντος διαπραγματεύεται το ίδιο πρόβλημα στα "Αριθμητικά"

"*Τον επιταχθέντα τετράγωνον διελείν εις δύο τετραγώνους*",

αλλά η λύση που δίνει βρίσκεται πιο κοντά στο σύγχρονο αλγεβρικό τρόπο σκέψης. Αυτό ακριβώς το πρόβλημα ήταν η αφορμή να ισχυριστεί ο P. Fermat (1601-1665) ότι η διοφαντική εξίσωση $x^{\nu}+y^{\nu}=z^{\nu}$ είναι αδύνατη, όταν ο ν είναι φυσικός μεγαλύτερος του 2, σημειώνοντας μάλιστα πάνω στο βιβλίο του Διόφαντου που μελετούσε: "έχω μια αληθινά θαυμάσια απόδειξη αυτής της πρότασης, αλλά το περιθώριο είναι πολύ στενό για να τη χωρέσει". Ο ισχυρισμός αυτός του Fermat αποδείχτηκε αληθής το 1994 από τον A. Wiles, αφού υπήρξε για 350 χρόνια ένα από τα διασημότερα άλυτα προβλήματα της Θεωρίας Αριθμών.
Η επίλυση διοφαντικών εξισώσεων βαθμού μεγαλύτερου του 2ου αποτελεί ένα ανοικτό μαθηματικό πρόβλημα, καθώς δεν έχουν βρεθεί γενικοί τύποι επίλυσης. Ο D. Hilbert διατύπωσε το 1900, ως ένα ζήτημα βασικής μαθηματικής έρευνας στη διάρκεια του 20ού αιώνα, την αναζήτηση ενός αλγόριθμου επίλυσης μιας διοφαντικής εξίσωσης με οποιοδήποτε αριθμό αγνώστων. Το 1970, ο Y. Matyasevich, σε ηλικία 22 χρόνων, απέδειξε ότι ένας τέτοιος αλγόριθμος δεν υπάρχει.

Επίλυση Γραμμικής Διοφαντικής Εξίσωσης

Έστω η εξίσωση $\alpha x+\beta y=\gamma$, όπου α,β,γ ακέραιοι με $\alpha\neq 0$ και $\beta\neq 0$. Αν αναζητούμε ακέραιες λύσεις της εξίσωσης αυτής, δηλαδή ζεύγη ακεραίων (x,y) που την επαληθεύουν, τότε λέμε ότι έχουμε να λύσουμε μια **γραμμική διοφαντική εξίσωση**.
Μερικές διοφαντικές εξισώσεις μπορεί να έχουν πολλές λύσεις, όπως, για παράδειγμα, η $3x+6y=18$, για την οποία μπορούμε να διαπιστώσουμε με αντικατάσταση ότι τα ζεύγη $(4,1)$, $(-6,6)$, $(10,-2)$ είναι ακέραιες λύσεις της.Υπάρχουν όμως διοφαντικές εξισώσεις που δεν έχουν καμιά λύση. Για παράδειγμα, η διοφαντική εξίσωση $2x+6y=13$ δεν έχει καμιά λύση, αφού για όλες τις ακέραιες τιμές των x,y το πρώτο μέλος της είναι άρτιος αριθμός, ενώ το δεύτερο μέλος της είναι περιττός αριθμός. Το θεώρημα που ακολουθεί δίνει απάντηση στο ερώτημα πότε μια διοφαντική εξίσωση έχει λύση, και αν έχει, πόσες είναι αυτές οι λύσεις.

ΘΕΩΡΗΜΑ 10

Η γραμμική διοφαντική εξίσωση $\alpha x + \beta y = \gamma$ έχει λύση, αν και μόνο αν ο μέγιστος κοινός διαιρέτης δ των α, β διαιρεί το γ.

Αν η εξίσωση αυτή έχει μια λύση (x_0, y_0), τότε έχει άπειρες λύσεις (x, y), που δίνονται από τους τύπους

$$x = x_0 + \frac{\beta}{\delta}t, \quad y = y_0 - \frac{\alpha}{\delta}t, \quad \text{όπου } t \in \mathbf{Z}.$$

ΑΠΟΔΕΙΞΗ

- Έστω ότι $\delta|\gamma$,δηλαδή ότι $\gamma = \mu\delta$, $\mu \in \mathbf{Z}$. Γνωρίζουμε ότι για τον $\delta = (\alpha, \beta)$ υπάρχουν ακέραιοι κ, λ, τέτοιοι, ώστε

$$\kappa\alpha + \lambda\beta = \delta. \qquad (1)$$

Πολλαπλασιάζοντας τα μέλη της (1) με μ βρίσκουμε $\mu\kappa\alpha + \mu\lambda\beta = \mu\delta$, δηλαδή

$$\alpha(\kappa\mu) + \beta(\lambda\mu) = \gamma.$$

Άρα, το ζεύγος $(\kappa\mu, \lambda\mu)$ είναι μια λύση της εξίσωσης.

Αντιστρόφως, αν (x_0, y_0) είναι μια λύση της διοφαντικής εξίσωσης, τότε θα ισχύει $\alpha x_0 + \beta y_0 = \gamma$. Επειδή $\delta|\alpha$ και $\delta|\beta$, συμπεραίνουμε ότι $\delta|(\alpha x_0 + \beta y_0)$, δηλαδή $\delta|\gamma$.

- Έστω (x_0, y_0) μια λύση της διοφαντικής εξίσωσης $\alpha x + \beta y = \gamma$. Τότε θα ισχύει

$$\alpha x_0 + \beta y_0 = \gamma.$$

Αν (x', y') είναι μια άλλη λύση της διοφαντικής εξίσωσης $\alpha x + \beta y = \gamma$, τότε θα ισχύει

$$\alpha x' + \beta y' = \gamma,$$

οπότε με αφαίρεση των δυο ισοτήτων κατά μέλη παίρνουμε $\alpha(x_0 - x') + \beta(y_0 - y') = 0$ ή ισοδύναμα

$$\alpha(x_0 - x') = -\beta(y_0 - y'). \qquad (2)$$

Επειδή $\delta = (\alpha, \beta)$, οι αριθμοί $\frac{\alpha}{\delta} = \rho$ και $\frac{\beta}{\delta} = \sigma$ είναι πρώτοι μεταξύ τους. Από την (2), με διαίρεση και των δύο μελών της με δ, έχουμε

$$\rho(x_0 - x') = -\sigma(y_0 - y'),$$

Έτσι, ο ρ διαιρεί το πρώτο μέλος της ισότητας, οπότε θα διαιρεί και το δεύτερο και επειδή είναι πρώτος προς το σ, θα διαιρεί τον ακέραιο $y_0 - y'$. Επομένως, θα υπάρχει ακέραιος t, τέτοιος, ώστε $y_0 - y' = \rho t$, δηλαδή $y_0 - y' = \frac{\alpha}{\delta}t$. Άρα $y' = y_0 - \frac{\alpha}{\delta}t$, οπότε, λόγω της (2), θα είναι $x' = x_0 + \frac{\beta}{\delta}t$.

Αντιστρόφως, για κάθε $t \in \mathbf{Z}$, ισχύει

$$\alpha\left(x_0 + \frac{\beta}{\delta}t\right) + \beta\left(y_0 - \frac{\alpha}{\delta}t\right) = \alpha x_0 + \beta y_0 + \alpha\frac{\beta}{\delta}t - \beta\frac{\alpha}{\delta}t = \gamma,$$

που σημαίνει ότι και το ζεύγος $\left(x_0 + \frac{\beta}{\delta}t, y_0 - \frac{\alpha}{\delta}t\right)$, $t \in \mathbf{Z}$ είναι λύση της εξίσωσης.

Ώστε, αν μια διοφαντική εξίσωση έχει μια λύση (x_0, y_0), τότε έχει άπειρες λύσεις της μορφής $\left(x_0 + \frac{\beta}{\delta}t,\ y_0 - \frac{\alpha}{\delta}t\right)$, $t \in \mathbf{Z}$. ■

Στην περίπτωση που είναι $(\alpha,\delta)=1$, οι παραπάνω τύποι παίρνουν τη μορφή:

$$x = x_0 + \beta t,\ y = y_0 - \alpha t,\ t \in \mathbf{Z}.$$

Η γεωμετρική ερμηνεία του παραπάνω θεωρήματος προκύπτει, αν λάβουμε υπόψη ότι κάθε εξίσωση της μορφής $\alpha x + \beta y = \gamma$, με $\alpha \neq 0$ ή $\beta \neq 0$, παριστάνει στο επίπεδο μια ευθεία. Στην περίπτωση που $\alpha,\beta,\gamma \in \mathbf{Z}$, η ευθεία αυτή διέρχεται από άπειρα σημεία με ακέραιες συντεταγμένες, αν και μόνο αν ο $\delta \mid \gamma$, όπου $\delta = (\alpha,\beta)$.

Για παράδειγμα, η ευθεία $2x + 3y = 1$ διέρχεται από άπειρο πλήθος σημείων με ακέραιες συντεταγμένες, ενώ η $6x + 4y = 5$ δε διέρχεται από κανένα τέτοιο σημείο.

ΕΦΑΡΜΟΓΗ

Κάποιος οδηγός που χρειάζεται κέρματα, για να ρίξει στο μηχάνημα στάθμευσης (parking), ζητάει από τον περιπτερά να του ανταλλάξει ένα χιλιάρικο με κέρματα των 100 δραχμών και των 50 δραχμών. Με πόσους τρόπους μπορεί να γίνει η ανταλλαγή, αν ο οδηγός θέλει οπωσδήποτε και κατοστάρικα και πενηντάρικα;

ΛΥΣΗ

Αν η ανταλλαγή μπορεί να γίνει με x κατοστάρικα και y πενηντάρικα, τότε

$$100x+50y=1000 \text{ ή}$$
$$2x+y=20. \qquad (1)$$

Αναζητούμε προφανώς τις ακέραιες και θετικές λύσεις της (1). Επειδή $(2,1)=1$ και $1|20$, η εξίσωση έχει ακέραιες λύσεις. Για να βρούμε το σύνολο των λύσεών της, πρέπει να βρούμε μια μερική λύση (x_0,y_0) της εξίσωσης ή, όπως λέμε, μια *ειδική λύση* της εξίσωσης.
Εκφράζουμε γραμμικά το Μ.Κ.Δ. των 2 και 1 και έχουμε

$$2(1)+1(-1)=1. \qquad (2)$$

Πολλαπλασιάζουμε τα μέλη της (2) με 20 και έχουμε $2(20)+1(-20)=20$, που σημαίνει ότι $(x_0,y_0)=(20,-20)$. Επομένως, οι ακέραιες λύσεις της εξίσωσης (1) δίνονται από τους τύπους:

$$x=20+1\cdot t, \quad y=-20-2\cdot t, \quad t\in\mathbf{Z}.$$

Από τις λύσεις αυτές πρέπει να βρούμε εκείνες για τις οποίες ισχύει $x>0$ και $y>0$, δηλαδή πρέπει να βρούμε πού συναληθεύουν οι ανισώσεις

$$20+1\cdot t>0 \quad \text{και} \quad -20-2\cdot t>0, \ t\in\mathbf{Z}.$$

Από την επίλυση του συστήματος των ανισώσεων προκύπτει ότι $-20<t<-10$, $t\in\mathbf{Z}$. Επομένως, $t=-19,-18,-17,-16,-15,-14,-13,-12,-11$ και οι αντίστοιχες τιμές των x και y φαίνονται στον παρακάτω πίνακα:

x	1	2	3	4	5	6	7	8	9
y	18	16	14	12	10	8	6	4	2

ΑΣΚΗΣΕΙΣ

Α΄ ΟΜΑΔΑΣ

1. Ποιες από τις παρακάτω εξισώσεις έχουν ακέραιες λύσεις;
(i) $4x+6y=5$ (ii) $4x-6y=2$
(iii) $3x+5y=\kappa$, $\kappa\in\mathbf{Z}$ (iv) $\kappa x+(\kappa+1)y=\lambda$, $\kappa,\lambda\in\mathbf{Z}$
(v) $2\kappa x+4y=2\lambda+1$, $\kappa,\lambda\in\mathbf{Z}$.

2. Να βρείτε τις ακέραιες λύσεις των εξισώσεων
(i) $2x+3y=5$, (ii) $6x-4y=8$ (iii) $7x-5y=19$, (iv) $5x-3y=7$.

3. Να βρείτε τις θετικές ακέραιες λύσεις των εξισώσεων
(i) $111x+78y=300$, (ii) $47x-31y=78$.

4. Να αποδείξετε ότι οι παρακάτω εξισώσεις δεν έχουν θετικές ακέραιες λύσεις:
(i) $3x+5y=-15$, (ii) $111x+78y=50$, (iii) $5x+7y=5$.

5. Με ποιους τρόπους μπορούμε να αλλάξουμε ένα νόμισμα 10.000 δραχμών με νομίσματα των 1.000 και 500 δραχμών;

Β΄ ΟΜΑΔΑΣ

1. Ένας καταστηματάρχης παραγγέλνει 19 μεγάλα και 3 μικρά πακέτα συσκευασίας με σαπούνια του ίδιου τύπου. Όταν όμως πήρε την παραγγελία, είδε έκπληκτος ότι η συσκευασία είχε καταστραφεί και τα σαπούνια ήταν σκόρπια στο κοντέινερ. Μπορείτε να τον βοηθήσετε να τα τακτοποιήσει με τον τρόπο που ήταν αρχικά συσκευασμένα, αν ξέρετε ότι το πλήθος των σαπουνιών είναι 224;

2. Να γράψετε τον αριθμό 100 ως άθροισμα δύο προσθετέων, έτσι ώστε ο ένας να είναι πολλαπλάσιο του 7 και ο άλλος πολλαπλάσιο του 11. (Euler 1770).

3. Να βρείτε την ελάχιστη δυνατή απόσταση ανάμεσα σε δύο σημεία, με ακέραιες συντεταγμένες, της ευθείας με εξίσωση $\alpha x+\beta y=\gamma$, όταν $\alpha,\beta,\gamma\in\mathbf{Z}$ με $(\alpha,\beta)|\gamma$.

4. Έστω $\alpha,\beta\in\mathbf{N}^*$ με $(\alpha,\beta)=1$. Να αποδείξετε ότι
(i) Η εξίσωση $\alpha x+\beta y=\alpha\beta$ δεν έχει θετικές ακέραιες λύσεις.
(ii) Η εξίσωση $\alpha x+\beta y=2\alpha\beta$ έχει μία μόνο θετική ακέραια λύση.

5. Να βρείτε δύο κλάσματα με παρονομαστές 7 και 13 και με άθροισμα $\frac{33}{91}$.

4.7 ΙΣΟΫΠΟΛΟΙΠΟΙ ΑΡΙΘΜΟΙ

Το ζήτημα της διαιρετότητας των ακεραίων είναι κυρίαρχο θέμα στη Θεωρία των Αριθμών. Μια έννοια που βοηθάει στη μελέτη και επίλυση προβλημάτων διαιρετότητας είναι η έννοια των **ισοϋπόλοιπων αριθμών**. Για να γίνει αντιληπτή η έννοια αυτή, ας εξετάσουμε, για παράδειγμα, τα υπόλοιπα των διαιρέσεων των ακεραίων με τον αριθμό 5.
Από την ταυτότητα της αλγοριθμικής διαίρεσης γνωρίζουμε ότι το υπόλοιπο της διαίρεσης ενός ακεραίου με το 5 είναι ένας από τους πέντε ακεραίους 0,1,2,3 και 4. Έτσι έχουμε

$0=0\cdot5+0$	$5=1\cdot5+0$	$-1=-1\cdot5+4$
$1=0\cdot5+1$	$6=1\cdot5+1$	$-2=-1\cdot5+3$
$2=0\cdot5+2$	$7=1\cdot5+2$	$-3=-1\cdot5+2$
$3=0\cdot5+3$	$8=1\cdot5+3$	$-4=-1\cdot5+1$
$4=0\cdot5+4$	$9=1\cdot5+4$	$-5=-1\cdot5+0$
	…….	$-6=-2\cdot5+4$
		$-7=-2\cdot5+3$
		…….

Παρατηρούμε ότι οι αριθμοί $2,7,-3$ διαιρούμενοι με 5 αφήνουν το ίδιο υπόλοιπο 2. Λέμε ότι οι αριθμοί αυτοί είναι *ισοϋπόλοιποι με μέτρο 5*. Ομοίως, λέμε ότι και οι αριθμοί $4,9,-1,-6$ είναι *ισοϋπόλοιποι με μέτρο 5*, αφού διαιρούμενοι με 5 αφήνουν το ίδιο υπόλοιπο 4. Γενικότερα, έχουμε:

ΟΡΙΣΜΟΣ

Έστω m ένας θετικός ακέραιος. Δύο ακέραιοι α και β λέγονται **ισοϋπόλοιποι με μέτρο m**, όταν διαιρούμενοι με m αφήνουν το ίδιο υπόλοιπο.

Για να δηλώσουμε ότι οι α και β είναι ισοϋπόλοιποι με μέτρο m, γράφουμε

$$\alpha \equiv \beta (\mathrm{mod}\, m)$$

και διαβάζουμε "α ισοϋπόλοιπος του β μόντουλο m". Αν ο ακέραιος α δεν είναι ισοϋπόλοιπος του β μόντουλο m, γράφουμε $\alpha \not\equiv \beta (\mathrm{mod}\, m)$. Έτσι, $22 \equiv 2 (\mathrm{mod}\, 5)$, ενώ $8 \not\equiv 5 (\mathrm{mod}\, 5)$.

Αν το υπόλοιπο της ευκλείδειας διαίρεσης του α με τον m είναι υ, τότε προφανώς ισχύει

$$\alpha \equiv \upsilon (\mathrm{mod}\, m).$$

Από την ισότητα της ευκλείδειας διαίρεσης προκύπτει το επόμενο θεώρημα, με το οποίο μπορούμε να διαπιστώσουμε αν δυο αριθμοί είναι ισοϋπόλοιποι.

ΘΕΩΡΗΜΑ 11

$\alpha \equiv \beta (\mathrm{mod}\, m)$, αν και μόνον αν $m | (\alpha - \beta)$.

ΑΠΟΔΕΙΞΗ

Αν $\alpha \equiv \beta (\mathrm{mod}\, m)$, τότε από τις ευκλείδειες διαιρέσεις των α και β με το m έχουμε $\alpha = \kappa m + \upsilon$, $\beta = \lambda m + \upsilon$. Επομένως, $\alpha - \beta = (\kappa - \lambda) m$, που σημαίνει ότι $m | (\alpha - \beta)$.

Αντιστρόφως, αν $m|\alpha-\beta$, τότε $\alpha-\beta=\rho m$, δηλαδή $\alpha=\beta+\rho m$ για κάποιο ακέραιο ρ. Αν ο β διαιρούμενος με τον m δίνει πηλίκο κ και υπόλοιπο υ, τότε $\beta=\kappa m+\upsilon$, $0\le\upsilon<m$. Επομένως, $\alpha=\kappa m+\upsilon+\rho m=(\kappa+\rho)m+\upsilon$, που σημαίνει ότι ο α διαιρούμενος με m δίνει υπόλοιπο επίσης υ. ■

Το συμβολισμό $\alpha\equiv\beta(\mathrm{mod}\,m)$ τον εισήγαγε ο Gauss(1777-1855). Όπως εξήγησε ο ίδιος, υιοθέτησε το σύμβολο "≡", επειδή η σχέση $\alpha\equiv\beta(\mathrm{mod}\,m)$ έχει ανάλογες ιδιότητες με την ισότητα.
Πράγματι, ως άμεσες συνέπειες του ορισμού των ισοϋπόλοιπων αριθμών προκύπτουν οι ιδιότητες:

- $\alpha\equiv\alpha(\mathrm{mod}\,m)$ (ανακλαστική)
- Αν $\alpha\equiv\beta(\mathrm{mod}\,m)$, τότε $\beta\equiv\alpha(\mathrm{mod}\,m)$ (συμμετρική)
- Αν $\alpha\equiv\beta(\mathrm{mod}\,m)$ και $\beta\equiv\gamma(\mathrm{mod}\,m)$, τότε $\alpha\equiv\gamma(\mathrm{mod}\,m)$ (μεταβατική).

Επίσης, ισχύει το επόμενο θεώρημα:

ΘΕΩΡΗΜΑ 12

Αν $\alpha\equiv\beta(\mathrm{mod}\,m)$ και $\gamma\equiv\delta(\mathrm{mod}\,m)$, τότε

- $\alpha+\gamma\equiv\beta+\delta(\mathrm{mod}\,m)$
- $\alpha-\gamma\equiv\beta-\delta(\mathrm{mod}\,m)$
- $\alpha\cdot\gamma\equiv\beta\cdot\delta(\mathrm{mod}\,m)$.

ΑΠΟΔΕΙΞΗ

Έχουμε $\alpha-\beta=\kappa m$ και $\gamma-\delta=\lambda m$, όπου κ,λ ακέραιοι. Επομένως:
$(\alpha+\gamma)-(\beta+\delta)=(\alpha-\beta)+(\gamma-\delta)=\kappa m+\lambda m=(\kappa+\lambda)m$, που σημαίνει ότι

$$\alpha+\gamma\equiv\beta+\delta(\mathrm{mod}\,m)$$

$(\alpha-\gamma)-(\beta-\delta)=(\alpha-\beta)-(\gamma-\delta)=\kappa m-\lambda m=(\kappa-\lambda)m$, που σημαίνει ότι

$$\alpha-\gamma\equiv\beta-\delta(\mathrm{mod}\,m)$$

$(\alpha\gamma-\beta\delta)=\alpha\gamma-\beta\gamma+\beta\gamma-\beta\delta=(\alpha-\beta)\gamma-(\gamma-\delta)\beta=\kappa m\gamma-\lambda m\beta=(\kappa\gamma-\lambda\beta)m$, που σημαίνει ότι

$$\alpha\gamma\equiv\beta\delta(\mathrm{mod}\,m).$$ ■

Η σχέση $\alpha\equiv\beta(\mathrm{mod}\,m)$ λέγεται **ισοτιμία**.

Ως άμεση συνέπεια του θεωρήματος προκύπτει ότι:

Αν $\alpha\equiv\beta(\mathrm{mod}\,m)$, τότε $\alpha+\gamma\equiv\beta+\gamma(\mathrm{mod}\,m)$ και $\alpha\cdot\gamma\equiv\beta\cdot\gamma(\mathrm{mod}\,m)$ για κάθε ακέραιο γ.

Το παραπάνω θεώρημα γενικεύεται και για περισσότερες από δύο ισοτιμίες.

Δηλαδή

Αν $\alpha_1 \equiv \beta_1 (\mathrm{mod} m)$, $\alpha_2 \equiv \beta_2 (\mathrm{mod} m), ..., \alpha_\nu \equiv \beta_\nu (\mathrm{mod} m)$, **τότε**

$$\alpha_1 + \alpha_2 + ... + \alpha_\nu \equiv \beta_1 + \beta_2 + ... + \beta_\nu (\mathrm{mod} m)$$

$$\alpha_1 \cdot \alpha_2 \cdot ... \cdot \alpha_\nu \equiv \beta_1 \cdot \beta_2 \cdot ... \cdot \beta_\nu (\mathrm{mod} m)$$

Ιδιαίτερα:

Αν $\alpha \equiv \beta (\mathrm{mod} m)$, **τότε** $\alpha^\nu \equiv \beta^\nu (\mathrm{mod} m)$.

Ενώ, με πολλαπλασιασμό των μελών μιας ισοτιμίας με τον ίδιο ακέραιο προκύπτει πάλι ισοτιμία, δεν ισχύει το ίδιο και για τη διαίρεση. Για παράδειγμα, αν διαιρέσουμε τα μέλη της ισοτιμίας $14 \equiv 8 (\mathrm{mod}\, 6)$ με 2, δεν προκύπτει ισοτιμία. Πράγματι, $7 \not\equiv 4 (\mathrm{mod}\, 6)$.

Οι ισοτιμίες εμφανίζονται συχνά στην καθημερινή μας ζωή. Για παράδειγμα, ο ωροδείκτης των ρολογιών δείχνει την ώρα modulo 12 και ο χιλιομετρικός δείκτης των αυτοκινήτων δείχνει τα χιλιόμετρα που έχουμε διανύσει modulo 100.000. Έτσι, όταν η ώρα είναι 18, το ρολόι δείχνει 6, που είναι το υπόλοιπο της διαίρεσης του 18 με το 12, και όταν ένα αυτοκίνητο έχει διανύσει συνολικά 245.000 km, δείχνει 45.000 km, που είναι το υπόλοιπο της διαίρεσης του 245.000 με το 100.000.

ΕΦΑΡΜΟΓΕΣ

1. **Έστω** $N = \alpha_\nu 10^\nu + \alpha_{\nu-1} 10^{\nu-1} + \alpha_{\nu-2} 10^{\nu-2} + ... + \alpha_1 10 + \alpha_0$ **η δεκαδική παράστα-ση ενός θετικού ακέραιου** N **και** $S = \alpha_\nu + \alpha_{\nu-1} + \alpha_{\nu-2} + ... + \alpha_1 + \alpha_0$ **το άθροι-σμα των ψηφίων του. Να αποδειχτούν τα κριτήρια διαιρετότητας:**

(i) $25 | N$ **, αν και μόνο αν** $25 | \alpha_1 10 + \alpha_0$**.**

(ii) $9 | N$ **, αν και μόνο αν** $9 | S$ **.**

ΑΠΟΔΕΙΞΗ

(i) Προφανώς, $25 | \alpha_\nu 10^\nu + \alpha_{\nu-1} 10^{\nu-1} + \alpha_{\nu-2} 10^{\nu-2} + ... + \alpha_2 10^2$. Επομένως,

$$\alpha_\nu 10^\nu + \alpha_{\nu-1} 10^{\nu-1} + \alpha_{\nu-2} 10^{\nu-2} + ... + \alpha_2 10^2 \equiv 0 (\mathrm{mod}\, 25)$$

$$\alpha_\nu 10^\nu + \alpha_{\nu-1} 10^{\nu-1} + \alpha_{\nu-2} 10^{\nu-2} + ... + \alpha_2 10^2 + \alpha_1 10 + \alpha_0 \equiv \alpha_1 10 + \alpha_0 (\mathrm{mod}\, 25).$$

Δηλαδή, ένας ακέραιος διαιρείται με 25, αν και μόνο αν το τελευταίο διψήφιο τμήμα του διαιρείται με 25.

(ii) Έχουμε διαδοχικά: $10\equiv 1(\mathrm{mod}\,9)$

$$10^{\kappa}\equiv 1^{\kappa}(\mathrm{mod}\,9),\ \text{για}\ \kappa=0,1,2,3,4,...,\nu$$

$$10^{\kappa}\equiv 1(\mathrm{mod}\,9)$$

$$\alpha_{\kappa}10^{\kappa}\equiv\alpha_{\kappa}(\mathrm{mod}\,9).$$

Επομένως, $\alpha_0\equiv\alpha_0(\mathrm{mod}\,9)$, $\alpha_1 10\equiv\alpha_1(\mathrm{mod}\,9),...,\alpha_{\nu}10^{\nu}\equiv\alpha_{\nu}(\mathrm{mod}\,9)$. Προσθέτουμε τις ισοτιμίες κατά μέλη και έχουμε:

$$\alpha_{\nu}10^{\nu}+\alpha_{\nu-1}10^{\nu-1}+\alpha_{\nu-2}10^{\nu-2}+...+\alpha_1 10+\alpha_0\equiv\alpha_{\nu}+\alpha_{\nu-1}+\alpha_{\nu-2}+...+\alpha_1+\alpha_0(\mathrm{mod}\,9),$$

δηλαδή $N\equiv S(\mathrm{mod}\,9)$.

2. Να βρεθεί το τελευταίο ψηφίο του αριθμού $3^{1999}+2^{1999}$

ΛΥΣΗ

Έχουμε διαδοχικά: $3+2\equiv 0(\mathrm{mod}\,5)$

$$3\equiv -2(\mathrm{mod}\,5)$$

$$3^{1999}\equiv(-2)^{1999}(\mathrm{mod}\,5)$$

$$3^{1999}\equiv -2^{1999}(\mathrm{mod}\,5).$$

Επομένως, $3^{1999}-(-2)^{1999}\equiv 0(\mathrm{mod}\,5)$, δηλαδή $3^{1999}+2^{1999}\equiv 0(\mathrm{mod}\,5)$.

Άρα $5|3^{1999}+2^{1999}$, που σημαίνει ότι ο αριθμός $3^{1999}+2^{1999}$ λήγει σε 0 ή σε 5. Όμως, ο αριθμός $3^{1999}+2^{1999}$ είναι περιττός ως άθροισμα ενός περιττού και ενός άρτιου και άρα λήγει σε 5.

ΑΣΚΗΣΕΙΣ

Α΄ ΟΜΑΔΑΣ

1. Δίνονται τα σύνολα $A=\{33,-17,23,35,41,-20\}$ και $B=\{0,1,2,3,4,5,6\}$.
Να αντιστοιχίσετε τα στοιχεία $\alpha\in A$ σε εκείνα τα στοιχεία $\beta\in B$ για τα οποία ισχύει $\beta\equiv\alpha(\mathrm{mod}7)$.

2. Ποιες από τις παρακάτω προτάσεις είναι αληθείς;

(i) $15\kappa+1\equiv 1(\mathrm{mod}3)$, $\kappa\in\mathbf{Z}$, (ii) $15\kappa+1\equiv -4(\mathrm{mod}5)$, $\kappa\in\mathbf{Z}$,

(iii) $\kappa^2+5\equiv 1(\mathrm{mod}4)$, $\kappa\in\mathbf{Z}$, (iv) $(m+1)^3\equiv 1(\mathrm{mod}m)$, $m\in\mathbf{N}^*$.

3. Να βρείτε τους διψήφιους θετικούς ακέραιους α για τους οποίους ισχύει $\alpha\equiv 6(\mathrm{mod}11)$.

4. Να βρείτε τους διψήφιους θετικούς ακέραιους α για τους οποίους ισχύει
(i) $\alpha\equiv 2(\mathrm{mod}3)$ και $\alpha\equiv 1(\mathrm{mod}4)$ (ii) $\alpha\equiv 3(\mathrm{mod}4)$ και $\alpha\equiv 4(\mathrm{mod}6)$.

5. Να βρείτε το υπόλοιπο της διαίρεσης
(i) του 2^{100} με τον 7, (ii) του 9^{100} με τον 8
(ii) του 3^{1998} με τον 7, (iv) του 5^{2004} με τον 26.

6. Να αποδείξετε ότι για κάθε $\nu\in\mathbf{N}^*$ ισχύει
(i) $8|(5^{2\nu}+7)$ (ii) $5|(2^{\nu+1}+3^{3\nu+1})$,
(iii) $15|(2^{4\nu}-1)$ (iv) $21|(2^{2\nu+4}+5^{2\nu+1})$

7. Να βρείτε
(i) το τελευταίο ψηφίο του αριθμού 3^{1998}
(ii) τα δύο τελευταία ψηφία του αριθμού 7^{2003}.

Β΄ ΟΜΑΔΑΣ

1. Να αποδείξετε ότι ο ακέραιος $3\alpha^2-1$, όπου $\alpha\in\mathbf{Z}$, δεν είναι ποτέ τετράγωνο ακεραίου.

2. Να αποδείξετε ότι για κάθε θετικό πρώτο $p>5$ ισχύει $10|(p^2-1)$ ή $10|(p^2+1)$.

3. Να βρείτε τις τιμές του $\alpha\in\mathbf{Z}$ για τις οποίες ισχύει $5|(\alpha^2+\alpha-6)$.

4. Να βρείτε τις τιμές του $x\in\mathbf{Z}$ για τις οποίες ισχύει $x\equiv 1(\mathrm{mod}2)$ και $x\equiv 2(\mathrm{mod}3)$.

5. Να αποδείξετε ότι για κάθε $\alpha\in\mathbf{Z}$ ισχύει
(i) $\alpha^3\equiv\alpha(\mathrm{mod}6)$ (ii) $\alpha^5\equiv\alpha(\mathrm{mod}10)$.

6. Έστω $\alpha,\beta\in\mathbf{Z}$ και $m,n\in\mathbf{N}^*$. Να αποδείξετε ότι
(i) Αν $\alpha\equiv\beta(\mathrm{mod}m)$ και $n|m$, τότε $\alpha\equiv\beta(\mathrm{mod}n)$
(ii) Αν $n\alpha\equiv n\beta(\mathrm{mod}m)$ και $(m,n)=1$, τότε $\alpha\equiv\beta(\mathrm{mod}m)$.

7. Αν $\alpha,\beta\in\mathbf{Z}$ και $m\in\mathbf{N}^*$ με $\alpha\equiv\beta(\mathrm{mod}m)$, να αποδείξετε ότι $(\alpha,m)=(\beta,m)$.

8. Να αποδείξετε ότι:
(i) $39|(53^{103}+103^{53})$, (ii) $7|(111^{333}+333^{111})$.

9. Να αποδείξετε ότι:
(i) Για κάθε θετικό ακέραιο α ισχύει $\alpha^2 \equiv 0$ ή 1 ή 4(mod5).
(ii) Οι αριθμοί $\sqrt{5\nu+2}$ και $\sqrt{5\nu+3}$ είναι άρρητοι.

10. Να αποδείξετε ότι για κάθε θετικό πρώτο $p>3$ ισχύει $p^2 \equiv 1(\text{mod}3)$ και στη συνέχεια να αποδείξετε ότι οι αριθμοί p^2+2 και $p_1^2+p_2^2+p_3^2$ είναι σύνθετοι για όλους τους θετικούς πρώτους p, p_1, p_2, p_3 που είναι μεγαλύτεροι από τον 3.

11. Αν p,q είναι θετικοί πρώτοι με $p>q\geq 5$, να αποδείξετε ότι $24|(p^2-q^2)$.

12. Να βρείτε το ψηφίο των μονάδων των αριθμών 77^{77} και 333^{333}.

13. Να αποδείξετε ότι ο αριθμός $2^{1999}+2^{1997}-1$ είναι σύνθετος.

ΓΕΝΙΚΕΣ ΑΣΚΗΣΕΙΣ

1. Να αποδείξετε ότι από ν διαδοχικούς ακεραίους ακριβώς ένας διαιρείται με το ν.

2. Να βρείτε τους θετικούς ακεραίους α,β,γ για τους οποίους ισχύει

$$\frac{\alpha+2}{8}=\frac{\beta+3}{6}=\frac{10}{\gamma+4}.$$

3. Να αποδείξετε ότι το άθροισμα $\nu\geq 2$ διαδοχικών περιττών φυσικών είναι σύνθετος αριθμός.

4. Έστω α,β δύο θετικοί ακέραιοι, με $(\alpha,\beta)=1$. Να αποδείξετε ότι

(i) $(\alpha^2+\beta^2,\ \alpha\beta)=1$ (ii) $\frac{\alpha}{\beta}+\frac{\beta}{\alpha}\notin \mathbf{N}^*$, αν $\alpha\neq\beta$.

5. (i) Έστω α,β θετικοί ακέραιοι. Να αποδείξετε ότι
- Αν $(\alpha,\beta)=1$, τότε $(\alpha+\beta,\alpha\beta)=1$.
- $(\alpha+\beta,[\alpha,\beta])=(\alpha,\beta)$.

(ii) Να βρείτε τους θετικούς ακεραίους α,β για τους οποίους ισχύει $\alpha+\beta=114$ και $[\alpha,\beta]=360$.

6. Έστω p,q δύο θετικοί πρώτοι, διαφορετικοί μεταξύ τους. Να αποδείξετε ότι τα στοιχεία του συνόλου $S=\{\kappa p+\lambda q|\kappa,\lambda\in\mathbf{N}^*$ με $1\leq\kappa\leq q$ και $1\leq\lambda\leq p\}$ είναι διαφορετικά ανά δύο.

7. (i) Να αποδείξετε ότι $2^v > 2v$ για κάθε θετικό ακέραιο $v \geq 3$.
(ii) Να βρείτε τις θετικές ακέραιες λύσεις της εξίσωσης $2^x = x^2$.

8. Δίνονται οι θετικοί ακέραιοι $\alpha, v \geq 2$. Να αποδείξετε ότι
(i) Αν ο $\alpha^v - 1$ είναι πρώτος, τότε $\alpha = 2$ και ο v είναι πρώτος.
(ii) Αν ο $\alpha^v + 1$ είναι πρώτος, τότε $v = 2^\kappa$ και ο α είναι πρώτος.

9. Να αποδείξετε ότι
(i) $\alpha^2 \equiv 0(\text{mod}8)$ ή $\alpha^2 \equiv 1(\text{mod}8)$ ή $\alpha^2 \equiv 4(\text{mod}8)$.
(ii) Η εξίσωση $x^2 + y^2 = 1998$ δεν έχει ακέραιες λύσεις.

10. (i) Να αποδείξετε ότι
$9^{10} \equiv 1(\text{mod}4)$, $9^{10} \equiv 1(\text{mod}25)$ και $9^{10} \equiv 1(\text{mod}100)$.
(ii) Να βρείτε τα δύο τελευταία ψηφία του 9^{2002}.

11. (i) Να βρείτε τους θετικούς ακέραιους $v > 2$ για τους οποίους ισχύει: $(v-2) | 2v$.
(ii) Να βρείτε τα ορθογώνια με ακέραια μήκη πλευρών, των οποίων το εμβαδόν και η περίμετρος είναι αριθμητικά ίσα.
(iii) Έστω ένα σημείο A ενός επιπέδου. Για ποιες τιμές του v ο χώρος γύρω από το A μπορεί να καλυφθεί με κανονικά v-γωνα, τα οποία δεν έχουν κοινά εσωτερικά τους σημεία.

12. Να βρείτε ο εμβαδόν του τετραγώνου που μπορεί να χωριστεί σε 25 μικρότερα τετράγωνα, από τα οποία τα 24 έχουν πλευρά ίση με 1, ενώ το ένα έχει πλευρά με μήκος ακέραιο αριθμό διαφορετικό από 1.

13. Μπορείτε να γράψετε μερικούς αριθμούς, χρησιμοποιώντας καθένα από τα δέκα ψηφία $0, 1, 2, ..., 8, 9$ μόνο μία φορά, ώστε το άθροισμα των αριθμών αυτών να είναι ίσο με 100.

14. Να βρείτε τους $\alpha, \beta \in \mathbf{N}^*$, με $\alpha > \beta$, σε καθεμιά από τις παρακάτω περιπτώσεις
(i) $\alpha + \beta = 10$ και $(\alpha, \beta) = 2$, (ii) $\alpha\beta = 96$ και $(\alpha, \beta) = 4$,
(iii) $\alpha\beta = 96$ και $[\alpha, \beta] = 24$ (iv) $(\alpha, \beta) = 4$ και $[\alpha, \beta] = 24$,
(v) $\alpha + \beta = 7(\alpha, \beta)$ και $[\alpha, \beta] = 60$.

15. Αν $\alpha, \beta \in \mathbf{N}^*$, να αποδείξετε ότι $(\alpha^2, \beta^2) = (\alpha, \beta)^2$.

16. Έστω $\alpha, \beta \in \mathbf{N}^*$ με $(\alpha, \beta) = 1$. Αν το γινόμενο των α και β είναι τετράγωνο φυσικού αριθμού, να αποδείξετε ότι καθένας από τους α και β είναι τετράγωνο φυσικού αριθμού.

ΕΡΩΤΗΣΕΙΣ ΚΑΤΑΝΟΗΣΗΣ

- Σε καθεμιά από τις παρακάτω περιπτώσεις να κυκλώσετε το γράμμα Α, αν ο ισχυρισμός είναι αληθής και το γράμμα Ψ, αν ο ισχυρισμός είναι ψευδής, αιτιολογώντας συγχρόνως την απάντησή σας.

1. Η παρακάτω ισότητα είναι η ταυτότητα της ευκλείδειας διαίρεσης του α με το β:

(i) $38=(-11)(-3)+5$, αν $\alpha=38$ και $\beta=-11$ Α Ψ

(ii) $38=(-3)(-11)+5$, αν $\alpha=38$ και $\beta=-3$ Α Ψ

(iii) $-47=7(-7)+2$, αν $\alpha=-47$ και $\beta=7$. Α Ψ

2. (i) Το άθροισμα δύο άρτιων είναι άρτιος Α Ψ

(ii) Το άθροισμα δύο περιττών είναι περιττός Α Ψ

(iii) Το άθροισμα 10 περιττών είναι περιττός Α Ψ

(iv) Η εξίσωση $x(x+1)=1999$ έχει ακέραια λύση Α Ψ

(v) Υπάρχει ακέραιος α που να μπορεί να πάρει συγχρόνως τις μορφές $\alpha=3k+1$ και $\alpha=3\lambda+2$, όπου $\kappa,\lambda\in\mathbf{Z}$. Α Ψ

3. (i) Αν $\alpha|\beta\gamma$, τότε $\alpha|\beta$ ή $\alpha|\gamma$ Α Ψ

(ii) Αν $\beta\gamma|\alpha$, τότε $\beta|\alpha$ και $\gamma|\alpha$ Α Ψ

(iii) Αν $\alpha|(\beta+\gamma)$ και $\alpha|\beta$, τότε $\alpha|\gamma$ Α Ψ

(iv) Αν $\alpha|\beta^2$, τότε $\alpha|\beta$. Α Ψ

4. (i) Αν $3|\alpha$ και $4|\alpha$, τότε $12|\alpha$ Α Ψ

(ii) Αν $4|\alpha$ και $6|\alpha$, τότε $24|\alpha$. Α Ψ

5. (i) Αν $(\alpha,\beta)=(\alpha,\gamma)$, τότε $[\alpha,\beta]=[\alpha,\gamma]$ Α Ψ

(ii) Αν $(\alpha,\beta)=(\alpha,\gamma)$, τότε $(\alpha,\beta,\gamma)=(\alpha,\beta)$. Α Ψ

6. Υπάρχουν $\alpha,\beta\in\mathbf{N}^*$, ώστε

(i) $\alpha+\beta=100$ και $(\alpha,\beta)=3$ Α Ψ

(ii) $\alpha+\beta=100$ και $(\alpha,\beta)=10$. Α Ψ

7. (i) Ο αριθμός 101 μπορεί να γραφεί ως άθροισμα δύο θετικών πρώτων Α Ψ

(ii) Αν $3|(\alpha^2+6\beta^2)$, τότε $3|\alpha$. Α Ψ

8. (i) Η εξίσωση $2x+4y=3$ έχει ακέραιες λύσεις Α Ψ

(ii) Η εξίσωση $x+2y=6$ έχει άπειρες θετικές ακέραιες λύσεις. Α Ψ

9. (i) Αν $2\alpha\equiv 2\beta(\mathrm{mod}4)$, τότε $\alpha\equiv\beta(\mathrm{mod}4)$ Α Ψ

(ii) Αν $2\alpha\equiv 2\beta(\mathrm{mod}3)$, τότε $\alpha\equiv\beta(\mathrm{mod}3)$ Α Ψ

(iii) Αν $\alpha^2\equiv 1(\mathrm{mod}3)$, τότε $\alpha\equiv 1(\mathrm{mod}3)$ ή $\alpha\equiv -1(\mathrm{mod}3)$. Α Ψ

- Να κυκλώσετε τη σωστή απάντηση σε καθεμιά από τις παρακάτω περιπτώσεις:

1. Αν $\alpha=4\cdot 6+x$ είναι η ταυτότητα της διαίρεσης του α με τον 4 και $\beta=(x+1)6+3$ είναι η ταυτότητα της διαίρεσης του β με τον $(x+1)$, τότε

$A: x=0$, $B: x=1$, $\Gamma: x=2$, $\Delta: x=3$.

2. Αν $\alpha=3\kappa+\upsilon$ είναι η ταυτότητα της διαίρεσης του α με τον 3 και ο α είναι άρτιος, τότε

A: κ περιττός και υ άρτιος B: κ άρτιος και υ περιττός

Γ: κ,υ άρτιοι ή κ,υ περιττοί

3. Αν $\delta=(4\nu+3, 4\nu-1)$, τότε

$A: \delta=4$, $B: \delta=2$, $\Gamma: \delta=1$, Δ: Ο δ εξαρτάται από το ν.

4. Αν ο αριθμός $\boxed{x}\,2722\,\boxed{x}$ διαιρείται με τον 12, τότε

$A: x=1$, $B: x=4$, $\Gamma: x=7$, $\Delta: x=2$.

5. Αν $(\alpha,\beta)=2^2\cdot 3$, $(\beta,\gamma)=2\cdot 3^2$ και $(\gamma,\alpha)=2\cdot 3\cdot 5$, τότε ο (α,β,γ) είναι

$A: 2^2\cdot 3^2\cdot 5$, $B: 2\cdot 3$, $\Gamma: 2$, $\Delta: 3$.

6. Αν ο ν είναι περιττός, τότε ο ακέραιος

$A: 9^\nu+1\equiv 0(\mathrm{mod}8)$, $B: 9^\nu+1\equiv 0(\mathrm{mod}3)$

$\Gamma: 9^\nu+1\equiv 0(\mathrm{mod}10)$, $\Delta: 9^\nu+1\equiv 0(\mathrm{mod}4)$.