ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

Ορισμός 1: Ένας ακέραιος $n>1$ καλείται πρώτος αν οι μόνοι θετικοί διαιρέτες του n είναι οι 1 και n. Αν ο ακέραιος $n>1$ δεν είναι πρώτος τότε ο n καλείται σύνθετος. □

Παρατήρηση 2:

i) Αν ο ακέραιος $n>1$ είναι σύνθετος τότε υπάρχει $\alpha\in\mathbb{Z}$ με $1<\alpha<n$ και $\alpha|n$ (δηλ. ο n έχει έναν τουλάχιστον διαιρέτη που ανήκει στο σύνολο $\{2,...,n-1\}$).

ii) Ο μοναδικός άρτιος πρώτος είναι το 2. Επομένως αν p πρώτος με $p>2$ τότε ο p είναι περιττός. Δεν ισχύει το αντίστροφο. Δηλαδή ένας περιττός φυσικός αριθμός μεγαλύτερος του 1 δεν είναι πάντα πρώτος. Π.χ. ο περιττός φυσικός αριθμός 5 είναι πρώτος, ενώ ο περιττός φυσικός αριθμός 9 δεν είναι πρώτος αφού $3|9$ και $3\neq 1,\ 3\neq 9$. □

Θεώρημα 3: Κάθε ακέραιος $n>1$ έχει έναν (τουλάχιστον) πρώτο διαιρέτη.

Απόδειξη: Έστω $n\in\mathbb{Z}$ με $n>1$. Θεωρούμε το σύνολο

$$A=\{m\in\mathbb{Z}/\ m>1 \text{ και } m|n\}$$

(δηλ. το A αποτελείται από όλους τους θετικούς διαιρέτες του n που είναι μεγαλύτεροι του 1). Προφανώς $n\in A$. Άρα $\varnothing\neq A\subseteq\mathbb{N}$ (δηλ. το A είναι ένα μη κενό υποσύνολο των φυσικών αριθμών). Συνεπώς το A περιέχει ελάχιστο στοιχείο. Αυτό σημαίνει ότι υπάρχει $p\in A$ τέτοιο ώστε $p\le m$ για κάθε $m\in A$. Θα δείξουμε ότι ο p είναι πρώτος αριθμός. Πράγματι:

Αφού $p\in A$ τότε $p>1$. Έστω τώρα ότι ο p είναι σύνθετος. Τότε (βλ. Παρατήρηση 2i) υπάρχει $\alpha\in\mathbb{Z}$ με $1<\alpha<p$ και $\alpha|p$. Επειδή $p\in A$ έχουμε ότι $p|n$. Επομένως $\alpha|n$. Άρα για το α έχουμε ότι $\alpha\in\mathbb{Z}$ με $\alpha>1$ και $\alpha|n$. Συνεπώς $\alpha\in A$. Άρα $p\le\alpha$ (αφού το p είναι το ελάχιστο στοιχείο του A). Αυτό όμως είναι άτοπο γιατί $\alpha<p$. Επομένως ο p δεν είναι σύνθετος. Συνεπώς ο p είναι πρώτος.

Επειδή $p\in A$ έχουμε αμέσως ότι $p|n$. Άρα ο p είναι πρώτος διαιρέτης του n. □

Παρατήρηση 4: Από το προηγούμενο Θεώρημα έπεται ότι κάθε ακέραιος $n>1$ είναι είτε πρώτος αριθμός είτε ένα γινόμενο πρώτων αριθμών. □

Θεώρημα 5 (Θεώρημα του Ευκλείδη): Υπάρχουν άπειροι πρώτοι αριθμοί.

Απόδειξη: Έστω ότι υπάρχουν πεπερασμένοι στο πλήθος πρώτοι αριθμοί, οι p_1, p_2, …, p_n ($n\in\mathbb{N}^*$). Θεωρούμε τον ακέραιο $m=p_1p_2...p_n+1$. Σύμφωνα με το Θεώρημα 3, ο m έχει έναν (τουλάχιστον) πρώτο διαιρέτη. Αυτός προφανώς θα είναι κάποιος από το σύνολο $\{p_1,p_2,...,p_n\}$. Δηλαδή υπάρχει $1\le i\le n$ με $p_i|m$. Όμως $p_i|p_1p_2...p_n$. Άρα $p_i|(m-p_1p_2...p_n)$. Δηλ. $p_i|1$. Αυτό όμως είναι άτοπο αφού $p_i>1$ διότι ο p_i είναι πρώτος. Επομένως το πλήθος των πρώτων αριθμών είναι άπειρο. □

Λήμμα 6: Έστω $\alpha,m,n\in\mathbb{Z}$ με $(\alpha,m)=1$ και $\alpha|mn$. Τότε $\alpha|n$.

Απόδειξη: Αφού $(\alpha,m)=1$ τότε υπάρχουν $x,y\in\mathbb{Z}$ τέτοια ώστε $1=\alpha x+my$. Επομένως $n=\alpha nx+mny$. Επειδή $\alpha|\alpha nx$ και $\alpha|mny$ (διότι από υπόθεση $\alpha|mn$), έπεται ότι $\alpha|(\alpha nx+mny)$. Άρα $\alpha|n$. □

Λήμμα 7: Έστω $\alpha,p\in\mathbb{Z}$ τέτοιοι ώστε ο p να είναι πρώτος και $p\not|\alpha$. Τότε $(p,\alpha)=1$.

Απόδειξη: Έστω $(p,\alpha)=d$. Τότε $d>0$ και $d|p$. Άρα (επειδή ο p είναι πρώτος) έχουμε $d=1$ ή $d=p$.

Έστω ότι $d=p$. Αφού $(p,\alpha)=d$ τότε $d|\alpha$. Άρα $p|\alpha$. Άτοπο. Επομένως $d=1$ και συνεπώς $(p,\alpha)=1$. □

Θεώρημα 8: Έστω $\alpha,b,p\in\mathbb{Z}$ τέτοιοι ώστε ο p να είναι πρώτος και $p|\alpha b$. Τότε $p|\alpha$ ή $p|b$.

Απόδειξη: Έστω ότι $p\not|\alpha$ (αν $p|\alpha$ τότε δεν έχουμε τίποτα να δείξουμε). Θα αποδείξουμε ότι $p|b$. Πράγματι:

Από το Λήμμα 7 έχουμε ότι $(p,\alpha)=1$. Τότε από το Λήμμα 6 έπεται αμέσως ότι $p|b$.

□

Παρατήρηση 9: Από το προηγούμενο Θεώρημα έπεται ότι αν ο p είναι πρώτος αριθμός και $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{Z}$ $(n \in \mathbb{N}^*)$ με $p \mid \alpha_1\alpha_2...\alpha_n$, τότε ο p διαιρεί έναν (τουλάχιστον) από τους α_1, α_2, …, α_n. □

Θεώρημα 10 (Θεμελιώδες Θεώρημα της Αριθμητικής): Κάθε ακέραιος $n > 1$ αναλύεται ως γινόμενο πρώτων παραγόντων κατά μοναδικό τρόπο (αν δεν ληφθεί υπόψη η σειρά των παραγόντων). □

Παρατήρηση 11: Από το Θεώρημα 10 έχουμε αμέσως ότι κάθε ακέραιος $n > 1$ γράφεται μονοσήμαντα στη μορφή

$$n = p_1^{r_1} p_2^{r_2} ... p_\kappa^{r_\kappa}$$

όπου $p_1 < p_2 < ... < p_\kappa$ πρώτοι αριθμοί και $r_1, r_2, ..., r_\kappa \in \mathbb{N}^*$ $(\kappa \in \mathbb{N}^*)$.

Επίσης από το Θεώρημα 6 έπεται ακόμη ότι και κάθε ακέραιος $n < -1$ γράφεται μονοσήμαντα στη μορφή

$$n = -p_1^{r_1} p_2^{r_2} ... p_\kappa^{r_\kappa}$$

όπου $p_1 < p_2 < ... < p_\kappa$ πρώτοι αριθμοί και $r_1, r_2, ..., r_\kappa \in \mathbb{N}^*$ $(\kappa \in \mathbb{N}^*)$.

Άρα κάθε ακέραιος $n \neq 0, \pm 1$ γράφεται μονοσήμαντα στη μορφή

$$n = \pm p_1^{r_1} p_2^{r_2} ... p_\kappa^{r_\kappa}$$

όπου $p_1 < p_2 < ... < p_\kappa$ πρώτοι αριθμοί και $r_1, r_2, ..., r_\kappa \in \mathbb{N}^*$ $(\kappa \in \mathbb{N}^*)$. Η μορφή αυτή του n καλείται **κανονική μορφή** του n. Η εύρεση της κανονικής μορφής ενός ακεραίου $n \neq 0, \pm 1$ περιγράφεται στο παρακάτω παράδειγμα:

Έστω $n = 126$. Βρίσκουμε τον πρώτο στη σειρά πρώτο αριθμό με τον οποίο διαιρείται το 126. Αυτός είναι το 2. Παρατηρούμε ότι $126 : 2 = 63$. Στη συνέχεια βρίσκουμε τον πρώτο στη σειρά πρώτο αριθμό με τον οποίο διαιρείται το 63. Αυτός είναι το 3. Παρατηρούμε ότι $63 : 3 = 21$. Συνεχίζουμε την προηγούμενη διαδικασία για το 21. Παρατηρούμε ότι $21 : 3 = 7$. Τελειώνουμε τη διαδικασία όταν θα καταλήξουμε σε πρώτο αριθμό (εδώ είναι το 7). Άρα $126 = 2 \cdot 3^2 \cdot 7$. Αυτή είναι η κανονική μορφή του 126. Η προηγούμενη διαδικασία συνήθως γράφεται σύντομα ως εξής:

$$\begin{array}{r|l} 126 & 2 \\ 63 & 3 \\ 21 & 3, \\ 7 & 7 \\ 1 & \end{array} \qquad 126 = 2 \cdot 3^2 \cdot 7$$

Αν ξεκινήσουμε με αρνητικό ακέραιο n, τότε εφαρμόζουμε την παραπάνω διαδικασία για τον $|n|$ και τότε η κανονική μορφή του n είναι η κανονική μορφή του $|n|$ με πρόσημο ' $-$ '. Δηλαδή αν $n = -126$ τότε η κανονική του μορφή είναι $-2 \cdot 3^2 \cdot 7$. □

Παρατήρηση 12: Έστω ακέραιος $n \neq 0, \pm 1$. Τότε από την προηγούμενη Παρατήρηση έχουμε ότι ο n γράφεται μονοσήμαντα στη μορφή $n = \pm p_1^{r_1} p_2^{r_2} ... p_\kappa^{r_\kappa}$, όπου $p_1 < p_2 < ... < p_\kappa$ πρώτοι αριθμοί και $r_1, r_2, ..., r_\kappa \in \mathbb{N}^*$ ($\kappa \in \mathbb{N}^*$). Τότε το σύνολο των διαιρετών του n είναι το σύνολο των αριθμών της μορφής:

$$\pm p_1^{\lambda_1} p_2^{\lambda_2} ... p_\kappa^{\lambda_\kappa}$$

όπου $\lambda_i \in \mathbb{Z}$ με $0 \leq \lambda_i \leq r_i$ για κάθε $i = 1, 2, ..., \kappa$. Οπότε το πλήθος των διαιρετών του n είναι $2(r_1 + 1)(r_2 + 1)...(r_\kappa + 1)$ (το πλήθος των θετικών διαιρετών του n είναι $(r_1 + 1)(r_2 + 1)...(r_\kappa + 1)$ και το πλήθος των αρνητικών διαιρετών του n είναι $(r_1 + 1)(r_2 + 1)...(r_\kappa + 1)$). □

Θεώρημα 13: Έστω ακέραιος $n > 1$. Τότε ο n είναι σύνθετος αν και μόνο αν υπάρχει p πρώτος διαιρέτης του n με $p \leq \sqrt{n}$.

Απόδειξη: (ευθύ)

Έστω ότι ο n είναι σύνθετος. Τότε (βλ. Παρατήρηση 2i)) υπάρχει $\alpha \in \mathbb{Z}$ με $1 < \alpha < n$ και $\alpha | n$. Αφού $\alpha | n$ τότε υπάρχει $b \in \mathbb{Z}$ με $n = \alpha b$. Από αυτό και το γεγονός ότι $1 < \alpha < n$ έχουμε αμέσως ότι $1 < b < n$. Επειδή $n = \alpha b$ τότε $\alpha \leq \sqrt{n}$ ή $b \leq \sqrt{n}$ (αν $\alpha > \sqrt{n}$ και $b > \sqrt{n}$ τότε θα είχαμε $\alpha b > \left(\sqrt{n}\right)^2 = n$ το οποίο είναι προφανώς άτοπο).

Ας υποθέσουμε – χωρίς βλάβη της γενικότητας – ότι $\alpha \leq \sqrt{n}$ (ακριβώς όμοια εργαζόμαστε αν $b \leq \sqrt{n}$). Από το Θεώρημα 3 έπεται ότι υπάρχει p πρώτος αριθμός

τέτοιος ώστε $p|\alpha$. Άρα $p \le \alpha$ και επομένως $p \le \sqrt{n}$. Επίσης επειδή $\alpha|n$ έχουμε και ότι $p|n$. Συνεπώς ο p είναι πρώτος διαιρέτης του n με $p \le \sqrt{n}$.

(αντίστροφο) Προφανές. □

Παρατήρηση 14: Για έναν ακέραιο $n > 1$, από το προηγούμενο Θεώρημα, έχουμε αμέσως τα εξής:

i) Ο n είναι πρώτος αν και μόνο αν δεν υπάρχει πρώτος αριθμός p τέτοιος ώστε $p|n$ και $p \le \sqrt{n}$.

ii) Ο n είναι πρώτος αν και μόνο αν για κάθε πρώτο αριθμό p με $p \le \sqrt{n}$ έχουμε ότι $p \nmid n$.

iii) Ο n είναι πρώτος αν και μόνο αν για κάθε πρώτο αριθμό p με $p|n$ έχουμε $p > \sqrt{n}$. □

Παρατήρηση 15 (Αλγόριθμος εύρεσης πρώτων αριθμών): Έστω ακέραιος $n > 1$. Τότε για να ελέγξουμε αν ο n είναι πρώτος μπορούμε να εφαρμόσουμε τον εξής αλγόριθμο:

I) Αν $n = 2$ ή $n = 3$ τότε ο n είναι προφανώς πρώτος αριθμός.

II) Αν $n \ge 4$ τότε υπολογίζουμε τη $\sqrt{n}$ και διακρίνουμε τις εξής περιπτώσεις:

i) Αν $\sqrt{n} \in \mathbb{N}$ τότε ο n είναι σύνθετος αριθμός αφού $n = \sqrt{n} \cdot \sqrt{n}$ με $\sqrt{n} \in \mathbb{Z}_+$ και $\sqrt{n} \ne 1, n$ διότι $n \ge 2$.

ii) Αν $\sqrt{n} \notin \mathbb{N}$ τότε θεωρούμε το σύνολο

$$A_n = \left\{ p \in \mathbb{Z} / \, p \text{ πρώτος και } p < \sqrt{n} \right\}$$

και έχουμε ελέγχουμε αν κάποιο από τα στοιχεία του A_n είναι διαιρέτης του n:

α) Αν κανένα στοιχείο του A_n δεν διαιρεί το n τότε (βλ. Παρατήρηση 14ii)) ο n είναι πρώτος αριθμός.

β) Αν υπάρχει στοιχείο του A_n το οποίο διαιρεί το n τότε (βλ. Θεώρημα 13) ο n είναι σύνθετος αριθμός.

Η δυσκολία του παραπάνω αλγορίθμου έγκειται στον υπολογισμό του συνόλου A_n για μεγάλα n.

Παράδειγμα:

Να εξεταστεί αν ο αριθμός 421 είναι πρώτος.

Επειδή $\sqrt{421} \simeq 20,52$, θα βρούμε το σύνολο $A_{421} = \left\{ p \in \mathbb{Z} / p \text{ πρώτος και } p < \sqrt{421} \right\}$.

Έχουμε προφανώς ότι $A_{421} = \{2,3,5,7,11,13,17,19\}$. Παρατηρούμε (απλώς υπολογισμός) ότι κανένα από τα στοιχεία του A_{421} δεν είναι διαιρέτης του 421. Άρα ο αριθμός 421 είναι πρώτος αριθμός. □

Παρατήρηση 16 (Το κόσκινο του Ερατοσθένη): Θεωρούμε ένα θετικό ακέραιο $n > 1$. Για να προσδιορίσουμε τους πρώτους αριθμούς του συνόλου $\{2,...,n\}$ εργαζόμαστε ως εξής:

i) Γράφουμε σε έναν πίνακα με αύξουσα σειρά τους φυσικούς από το 2 μέχρι το n.

ii) Κρατάμε το 2 (είναι ο πρώτος στη σειρά πρώτος αριθμός) και διαγράφουμε όλα τα πολλαπλάσια του 2 που υπάρχουν στον πίνακα.

iii) Στη συνέχεια κρατάμε το 3 (είναι ο δεύτερος στη σειρά πρώτος αριθμός και ο πρώτος στον πίνακα μετά το 2 που δεν έχει διαγραφεί) και διαγράφουμε όλα τα πολλαπλάσια του 3 που υπάρχουν στον πίνακα.

iv) Συνεχίζουμε με όμοιο τρόπο τη διαδικασία που περιγράψαμε στα i), ii) μέχρι τον πρώτο p για τον οποίο $p \le \sqrt{n}$ (στην αρχή κάθε βήματος ο πρώτος αριθμός που δεν έχει διαγραφεί μετά τον αριθμό του οποίου τα πολλαπλάσια διαγράψαμε στο προηγούμενο βήμα είναι ο επόμενος στη σειρά πρώτος αριθμός μετά από αυτόν που βρήκαμε στο προηγούμενο βήμα).

v) Οι αριθμοί του πίνακα που δεν έχουν διαγραφεί είναι οι πρώτοι αριθμοί του συνόλου $\{2,...,n\}$.

Η παραπάνω περιγραφείσα διαδικασία καλείται **κόσκινο του Ερατοσθένη** προς τιμή του αρχαίου Έλληνα μαθηματικού Ερατοσθένη που την ανακάλυψε.

Παράδειγμα: Εφαρμόζοντας την παραπάνω διαδικασία για $n = 50$ έχουμε ότι $\sqrt{50} \simeq 7,071$. Άρα οι πρώτοι που είναι μικρότεροι ή ίσοι του $\sqrt{50}$ είναι οι 2, 3, 5 και 7. Οπότε δημιουργείται ο πίνακας:

	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~~

Επομένως οι πρώτοι αριθμοί που είναι μικρότεροι ή ίσοι του 50 είναι οι 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 και 47. □

Θεώρημα 17 (μικρό Θεώρημα του Fermat): Για κάθε ακέραιο α και για κάθε πρώτο αριθμό p ισχύει:

$$p\left|\left(\alpha^{p}-\alpha\right)\right.$$ □

Πόρισμα 18: Έστω $\alpha\in\mathbb{Z}$ και p πρώτος αριθμός με $p\not|\alpha$. Τότε:

$$p\left|\left(\alpha^{p-1}-1\right)\right.$$

Απόδειξη: Από το προηγούμενο Θεώρημα έπεται ότι

$$p\left|\left(\alpha^{p}-\alpha\right)\right. \Rightarrow p\left|\alpha\left(\alpha^{p-1}-1\right)\right.$$

Τότε από το Θεώρημα 8 (αφού $p\not|\alpha$) έπεται αμέσως ότι $p\left|\left(\alpha^{p-1}-1\right)\right.$. □

Θεώρημα 19 (Θεώρημα του Wilson): Έστω $n\in\mathbb{Z}$ με $n>1$. Τότε ο n είναι πρώτος αν και μόνο αν $n\left|\left((n-1)!+1\right)\right.$ (όπου $(n-1)!=1\cdot 2\cdot\ldots\cdot(n-1)$). □

Ορισμός 20: Έστω δύο μη μηδενικοί ακέραιοι m και n. Ορίζουμε ως ελάχιστο κοινό πολλαπλάσιο των m και n το μικρότερο από τα κοινά θετικά πολλαπλάσια των m και n. Το ελάχιστο κοινό πολλαπλάσιο των m και n συμβολίζεται με $[m,n]$. □

Παρατήρηση 21: Έστω

$$\Pi_m=\left\{\kappa|m|\,/\,\kappa\in\mathbb{N}^*\right\}=\left\{|m|,2|m|,3|m|,\ldots\right\}$$

και

$$\Pi_n=\left\{\lambda|n|\,/\,\lambda\in\mathbb{N}^*\right\}=\left\{|n|,2|n|,3|n|,\ldots\right\}$$

Προφανώς $|m|\cdot|n| \in \Pi_m \cap \Pi_n$. Άρα $\varnothing \neq \Pi_m \cap \Pi_n \subseteq \mathbb{N}^*$. Συνεπώς το $\Pi_m \cap \Pi_n$ περιέχει ελάχιστο στοιχείο το οποίο είναι το ελάχιστο κοινό πολλαπλάσιο των m και n (δηλ. $[m,n] = \min(\Pi_m \cap \Pi_n)$). Επομένως το ελάχιστο κοινό πολλαπλάσιο $[m,n]$ των m και n είναι ο μοναδικός θετικός ακέραιος που έχει τις εξής ιδιότητες:

i) $[m,n] \in \Pi_m \cap \Pi_n$ (δηλ. το $[m,n]$ είναι κοινό θετικό πολλαπλάσιο των m και n).

ii) Αν $\alpha \in \Pi_m \cap \Pi_n$ τότε $[m,n] \leq \alpha$ (δηλ. το $[m,n]$ είναι μικρότερο ή ίσο από κάθε κοινό θετικό πολλαπλάσιο των m και n). □

<u>Θεώρημα 22:</u> Έστω $m,n \in \mathbb{Z}^*$. Τότε $(m,n)\cdot[m,n] = |m|\cdot|n|$. □

Από το Θεώρημα 22 έπεται αμέσως το εξής:

<u>Πόρισμα 23:</u> Έστω $m,n \in \mathbb{Z}^*$ με $(m,n)=1$. Τότε $[m,n] = |m|\cdot|n|$. □

<u>Θεώρημα 24:</u> Έστω $m,n \in \mathbb{Z}^*$ και $x \in \mathbb{Z}$. Το x είναι κοινό πολλαπλάσιο των m και n αν και μόνο αν το x είναι πολλαπλάσιο του $[m,n]$.

<u>Απόδειξη:</u> (<u>ευθύ</u>)

Έστω ότι το x είναι κοινό πολλαπλάσιο των m και n. Θα δείξουμε ότι το x είναι πολλαπλάσιο του $[m,n]$. <u>Πράγματι:</u>

Αφού το x είναι πολλαπλάσιο του m τότε υπάρχει $\kappa \in \mathbb{Z}$ τέτοιο ώστε $x = \kappa|m|$. Όμοια υπάρχει $\lambda \in \mathbb{Z}$ τέτοιο ώστε $x = \lambda|n|$. Έστω $(m,n) = d \underset{(m,n\in\mathbb{Z}^*)}{>} 0$. Τότε $d = (|m|,|n|)$ και άρα $\left(\frac{|m|}{d}, \frac{|n|}{d}\right) = 1$.

Τώρα έχουμε:

$$\kappa|m| = \lambda|n| \Leftrightarrow \kappa d\frac{|m|}{d} = \lambda d\frac{|n|}{d} \Leftrightarrow \kappa\frac{|m|}{d} = \lambda\frac{|n|}{d}$$

Όμως $\frac{|m|}{d} \Big| \kappa\frac{|m|}{d}$ (προφανές). Άρα $\frac{|m|}{d} \Big| \lambda\frac{|n|}{d}$ και επειδή $\left(\frac{|m|}{d}, \frac{|n|}{d}\right) = 1$, τότε (βλ. Λήμμα 6) $\frac{|m|}{d} \Big| \lambda$. Επομένως $\frac{\lambda d}{|m|} = \frac{\lambda}{\frac{|m|}{d}} \in \mathbb{Z}$. Άρα:

$$x = \lambda|n| = \frac{\lambda d}{|m|}\cdot\frac{|m|\cdot|n|}{d} = \frac{\lambda d}{|m|}\cdot\frac{|m|\cdot|n|}{(m,n)} \underset{(\Theta\text{εώρημα } 22)}{=} \frac{\lambda d}{|m|}\cdot[m,n]$$

Συνεπώς το x είναι πολλαπλάσιο του $[m,n]$ αφού, όπως δείξαμε παραπάνω, $\frac{\lambda d}{|m|}\in\mathbb{Z}$.

(αντίστροφο) Προφανές. □

Θεώρημα 25: Έστω p_1, p_2, …, p_κ ($\kappa\in\mathbb{N}^*$) πρώτοι αριθμοί και $m,n\in\mathbb{Z}^*$ με $m=\varepsilon_m p_1^{r_1}p_2^{r_2}...p_\kappa^{r_\kappa}$, $n=\varepsilon_n p_1^{\lambda_1}p_2^{\lambda_2}...p_\kappa^{\lambda_\kappa}$ όπου $\varepsilon_m,\varepsilon_n\in\{-1,+1\}$ και $r_1,r_2,...,r_\kappa,\lambda_1,\lambda_2,...,\lambda_\kappa\in\mathbb{N}$. Τότε:

i) $(m,n)=p_1^{c_1}p_2^{c_2}...p_\kappa^{c_\kappa}$ όπου $c_i=\min\{r_i,\lambda_i\}$ (= ο μικρότερος από τους r_i, λ_i) για κάθε $i=1,2,...,\kappa$.

ii) $[m,n]=p_1^{s_1}p_2^{s_2}...p_\kappa^{s_\kappa}$ όπου $s_i=\max\{r_i,\lambda_i\}$ (= ο μεγαλύτερος από τους r_i, λ_i) για κάθε $i=1,2,...,\kappa$. □

Παρατήρηση 26: Από το προηγούμενο Θεώρημα έπεται αμέσως ότι για να βρούμε τον μέγιστο κοινό διαιρέτη και το ελάχιστο κοινό πολλαπλάσιο δύο ακεραίων m, n με $m,n\neq 0,\pm 1$ μπορούμε να κάνουμε τα εξής:

i) Γράφουμε τους m, n στην κανονική τους μορφή (βλ. Παρατήρηση 11).

ii) Ο μέγιστος κοινός διαιρέτης των m, n είναι το γινόμενο των κοινών πρώτων παραγόντων (οι οποίοι εμφανίζονται στις κανονικές τους μορφές) υψωμένοι στις μικρότερες δυνάμεις. Αν δεν υπάρχουν κοινοί πρώτοι παράγοντες τότε (και μόνο τότε) ο μέγιστος κοινός διαιρέτης των m και n είναι το 1.

iii) Το ελάχιστο κοινό πολλαπλάσιο των m, n είναι το γινόμενο των κοινών και μη κοινών πρώτων παραγόντων (οι οποίοι εμφανίζονται στις κανονικές τους μορφές) υψωμένοι οι κοινοί παράγοντες στις μεγαλύτερες δυνάμεις.

Αν ένας από τους m, n είναι το 1 ή το –1, τότε $(m,n)=1$. Επίσης αν ένας από τους m, n είναι το 1 ή το –1, έστω ότι αυτό συμβαίνει για τον m, και $n\neq 0$ τότε $[m,n]=|n|$.

ΑΣΚΗΣΕΙΣ

1. Να βρείτε τους $\alpha,\beta\in\mathbb{Z}^*$ και τον πρώτο p σε κάθε μια από τις παρακάτω περιπτώσεις:

i) $(\alpha-\beta)(\alpha+\beta)=3$

ii) $\alpha^2-4=p$

iii) $(\alpha^2-1)p=15$

2. Έστω $n\in\mathbb{N}^*$ τέτοιος ώστε ο n δεν είναι τέλειο τετράγωνο. Να δείξετε ότι ο αριθμός $\sqrt{n}$ είναι άρρητος. Μπορείτε να γενικεύσετε το αποτέλεσμα;

3. Να βρείτε τον πρώτο αριθμό p για τον οποίο ισχύει:

i) $3p+1=n^2,\ n\in\mathbb{Z}.$

ii) $p=n^3-1,\ n\in\mathbb{Z}.$

iii) $p=n^3+1,\ n\in\mathbb{Z}.$

4. Έστω $\alpha,\nu,\kappa\in\mathbb{N}^*$ και πρώτος με $p\left|\alpha^{\nu}\right.$. Να αποδείξετε ότι $p^{\kappa}\left|\alpha^{\kappa}\right.$.

5. Έστω $\alpha,\beta\in\mathbb{Z}$ με $(\alpha,\beta)=1$. Να αποδείξετε τα εξής:

i) $(\alpha+\beta,\alpha\beta)=1$.

ii) $(\alpha^{\nu}+\beta^{\mu},\alpha^{\kappa}\beta^{\lambda})=1$, $\nu,\mu,\kappa,\lambda\in\mathbb{N}^*$.

6. Να αποδείξετε ότι είναι σύνθετοι οι αριθμοί:

i) n^4+4, όπου n φυσικός μεγαλύτερος του 1.

ii) 8^n+1, όπου $n\in\mathbb{N}^*$.

7. Να λύσετε στο $\mathbb{Z}$ τις εξισώσεις:

i) $x^3+x^2+x-3=0$

ii) $x^2+x+p=112$, όπου p πρώτος.

8. Έστω $\alpha,\beta,\nu\in\mathbb{N}^*$. Να αποδείξετε την ισοδυναμία:

$$\beta\left|\alpha\right. \Leftrightarrow \beta^{\nu}\left|\alpha^{\nu}\right.$$

9. Έστω $\alpha,\beta,\gamma,\delta\in\mathbb{Z}^*$ με $(\alpha,\beta)=(\gamma,\delta)=1$ και $\frac{\alpha}{\beta}+\frac{\gamma}{\delta}\in\mathbb{Z}$. Τότε $|\beta|=|\delta|$.

10. Δίνονται οι αριθμοί $\alpha=2\kappa+2$ και $\beta=6\kappa+7$, $\kappa\in\mathbb{Z}$. Να αποδείξετε ότι:

i) το υπόλοιπο της διαίρεσης του αριθμού $2\beta-\alpha$ με το 10 είναι 2.

ii) αν ο αριθμός κ είναι πολλαπλάσιο του 7, τότε και ο αριθμός $\alpha+\beta-2$ είναι πολλαπλάσιο του 7.

11. Δίνονται οι ακέραιοι αριθμοί $\beta=3\alpha+4$ και $\gamma=4\alpha+5$, $\alpha\in\mathbb{Z}$. Να αποδείξετε ότι:

i) ο αριθμός $\beta\gamma-(\beta+\gamma)$ είναι περιττός.

ii) αν $\alpha=3\kappa$, $\kappa\in\mathbb{Z}$, τότε ο αριθμός $\gamma^2-\beta^2$ είναι πολλαπλάσιο του 3.

12. Αν α είναι ένας άρτιος ακέραιος αριθμός, τότε να αποδείξετε ότι:

i) $4\left|\left[(\alpha+1)^2-1\right]\right.$

ii) $12\left|\left[\alpha^2+(\alpha+1)^2+(\alpha+3)^2-2\alpha+2\right]\right.$

13. Δίνεται ο αριθμός $A=9+9^2+9^3+...+9^{300}$. Να αποδείξετε ότι ο αριθμός Α διαιρείται με τους αριθμούς 3, 2, 5, 7, 9 και 13.

14. Αν $\alpha,\beta,\gamma\in\mathbb{Z}$ και $6\left|(\alpha+\beta+\gamma)\right.$, τότε να αποδείξετε ότι $6\left|(\alpha^3+\beta^3+\gamma^3)\right.$.

15. Να βρείτε τους ακέραιους αριθμούς x, y για τους οποίους ισχύει:

i) $(x-2)\left|11\right.$

ii) $xy=x+y$

iii) $12x+y(1-2x)=1$

16. Να αποδείξετε ότι

i) $25\left|(2^{n+4}+9\cdot3^{3n})\right.$, $n\in\mathbb{N}$

ii) $13\left|(4^{2n+1}+3^{n+2})\right.$, $n\in\mathbb{N}$

iii) $71\left|(15^n+3^{n+2}\cdot5^{n+1}+3^n\cdot5^{n+2})\right.$, $n\in\mathbb{N}$

17. Αν α, β είναι περιττοί ακέραιοι, να αποδείξετε ότι $8\left|(\alpha-\beta)(\alpha+\beta)\right.$.

18. Να βρείτε τους φυσικούς αριθμούς α για τους οποίους ισχύει $(\alpha+2)\left|(\alpha^2+4)\right.$.

19. Έστω α, β ακέραιοι με $7\left|(\alpha^2+\beta^2)\right.$. Να αποδείξετε ότι $7\left|\alpha\right.$ και $7\left|\beta\right.$.