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,...,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

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

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

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

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 (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 $A = p_1 p_2 \dots p_\nu + 1$. 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

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

ΑΠΟΔΕΙΞΗ

Έστω ότι $p \nmid \alpha$. 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 $p|\alpha_1\alpha_2\alpha_3 \dots \alpha_\nu$, τότε ο p διαιρεί έναν, τουλάχιστον, από τους παράγοντες του γινομένου".

ΘΕΩΡΗΜΑ

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:

ΠΟΡΙΣΜΑ:

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

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

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 ;;). Επομένως, $p|\alpha$ και $p|\beta$, που είναι άτοπο, αφού οι α και β είναι πρώτοι μεταξύ τους.