Διακριτά Μαθηματικά ΙΙ

Χρήστος Νομικός

Τμήμα Μηχανικών Η/Υ και Πληροφορικής
Πανεπιστήμιο Ιωαννίνων

MMXXIII

Περιεχόμενα

Περιεχόμενα

Ορισμός

Ένας ακέραιος αριθμός p ονομάζεται πρώτος αριθμός αν $p > 1$ και οι μόνοι θετικοί ακέραιοι που διαιρούν τον p είναι το 1 και ο p. Ένας ακέραιος αριθμός n ονομάζεται σύνθετος αν $n > 1$ και ο n δεν είναι πρώτος.

Παράδειγμα

Οι αριθμοί $2, 3, 5, 7, 31, 47, 101$ είναι πρώτοι αριθμοί.

Ο αριθμός 45 δεν είναι πρώτος επειδή διαιρείται (μεταξύ άλλων) με το 3. Το 45 είναι σύνθετος αριθμός.

Ο αριθμός 1 δεν είναι ούτε πρώτος ούτε σύνθετος αριθμός.

Με βάση τον ορισμό του πρώτου αριθμού, ο n είναι πρώτος αριθμός αν και μόνο αν δεν διαιρείται από κανέναν αριθμό k, με $1 < k < n$.

Με βάση την παραπάνω πρόταση, για να ελέγξουμε αν ένας αριθμός n είναι πρώτος, μπορούμε να εξετάσουμε το υπόλοιπο της διαίρεσής του με κάθε ακέραιο μεταξύ 2 και $n - 1$.

Στην πραγματικότητα το πλήθος των υποψήφιων διαρετών που θα πρέπει να εξετάσουμε είναι πολύ μικρότερο, όπως φαίνεται παρακάτω.

Λήμμα

Ένα ακέραιος αριθμός $n > 1$ είναι σύνθετος αν και μόνο αν διαιρείται από κάποιον ακέραιο αριθμό k, με $1 < k \leq \sqrt{n}$.

Απόδειξη

Έστω ένας ακέραιος αριθμός $n > 1$.

Απόδειξη (συνέχεια)

Αν ο n είναι σύνθετος αριθμός, τότε υπάρχει κάποιος ακέραιος αριθμός d, $1 < d < n$ τέτοιος ώστε $d \mid n$.

Αυτό συνεπάγεται ότι υπάρχει κάποιος ακέραιος q τέτοιος ώστε $q \cdot d = n$. Παρατηρούμε ότι ισχύει επίσης $q \mid n$.

Επειδη $1 < d < n$ θα πρέπει να ισχύει το ίδιο και για το αριθμό q. Άρα $1 < q < n$.

Συνεπώς οι d και q είναι διαιρέτες του n, μεγαλύτεροι από το 1 και μικρότεροι από το n.

Απόδειξη (συνέχεια)

Αν $d > \sqrt{n}$ και $q > \sqrt{n}$, τότε $q \cdot d > \sqrt{n} \cdot \sqrt{n} = n$. Αυτό είναι αδύνατο, καθώς $q \cdot d = n$

Συνεπώς θα πρέπει $d \leq \sqrt{n}$ ή $q \leq \sqrt{n}$.

Άρα ο αρίθμός $k = min(d, q)$ διαιρεί τον n και ισχύει $1 < k \leq \sqrt{n}$.

Απόδειξη (συνέχεια)

Αν ο n δεν είναι σύνθετος αριθμός, τότε είναι πρώτος αριθμός.

Συνεπώς ο n δεν διαιρείται από κανέναν ακέραιο αριθμό k με $1 < k < n$.

Επειδή $n > 1$ και άρα $\sqrt{n} < n$, η παραπάνω πρόταση συνεπάγεται ότι ο n δεν διαιρείται από κανέναν ακέραιο αριθμό k με $1 < k \leq \sqrt{n}$. □

Πόρισμα

Ένα ακέραιος αριθμός $n > 1$ είναι πρώτος αν και μόνο αν δεν διαιρείται από κανέναν ακέραιο αριθμό k, με $1 < k \leq \sqrt{n}$.

Λήμμα

Κάθε ακέραιος αριθμός $n > 1$ είτε είναι πρώτος αριθμός είτε διαιρείται από έναν πρώτο αριθμό $p < n$.

Απόδειξη

Θα αποδείξουμε το θεώρημα με ισχυρή επαγωγή στο n.

Για $n = 2$ η πρόταση αληθεύει, καθώς το 2 είναι πρώτος αριθμός.

Υποθέτουμε ότι η πρόταση αληθεύει για $2 \leq n \leq k$.

Απόδειξη (συνέχεια)

Αν το $k+1$ είναι πρώτος αριθμός, τότε η πρόταση αληθεύει για το $k+1$.

Αν το $k+1$ δεν είναι πρώτος αριθμός, τότε διαιρείται μέ κάποιον αριθμό d, όπου $2 \leq d \leq k$.

- Αν το d είναι πρώτος αριθμός, τότε η πρόταση αληθεύει για το $k+1$.
- Αν το d δεν είναι πρώτος αριθμός, τότε από την επαγωγική υπόθεση υπάρχει κάποιος πρώτος αριθμός $p < d$ ο οποίος διαιρεί το d. Επειδή $p \mid d$ και $d \mid n$, ισχύει επίσης $p \mid n$. Επιπλέον $p < d < n$. Συνεπώς και σε αυτή την περίπτωση η πρόταση αληθεύει για το $k+1$.

Απόδειξη (συνέχεια)

Συνεπώς το $k+1$ είτε είναι πρώτος αριθμός είτε διαιρείται από έναν πρώτο αριθμό μικρότερο του $k+1$.

Άρα η πρόταση ισχύει για κάθε $n > 1$. □

Θεώρημα

Ένα ακέραιος αριθμός $n > 1$ είναι σύνθετος αν και μόνο αν διαιρείται από έναν πρώτο αριθμό p, με $1 < p \leq \sqrt{n}$.

Απόδειξη

Έστω ένας ακέραιος αριθμός $n > 1$.

Απόδειξη (συνέχεια)

Αν ο n είναι σύνθετος αριθμός, τότε διαιρείται από ένα ακέραιο αριθμό k τέτοιον ώστε $1 < k \leq \sqrt{n}$.

- Αν ο k είναι πρώτος αριθμός τότε ο ισχυρισμός ισχύει για $p = k$.
- Αν ο k δεν είναι πρώτος αριθμός, τότε υπάρχει κάποιος πρώτος αριθμός $p < k$, ο οποίο διαιρεί το k. Επειδή $p \mid k$ και $k \mid n$, ισχύει $p \mid n$. Επιπλέον $1 < p < k \leq \sqrt{n}$

Συνεπώς σε κάθε περίπτωση ο n διαιρείται από έναν πρώτο αριθμό p, με $1 < p \leq \sqrt{n}$.

Απόδειξη (συνέχεια)

Αν ο n είναι δεν είναι σύνθετος αριθμός, τότε δεν διαιρείται από ένα ακέραιο αριθμό k με $1 < k \leq \sqrt{n}$.

Αυτό προφανώς συνεπάγεται ότι δεν διαιρείται με κανέναν πρώτο αριθμό στο ίδιο διάστημα. □

Πόρισμα

Ένα ακέραιος αριθμός $n > 1$ είναι πρώτος αριθμός αν και μόνο αν δεν διαιρείται με κανέναν πρώτο αριθμό p, με $1 < p \leq \sqrt{n}$.

Παράδειγμα

Ο αριθμός 103 είναι πρώτος αριθμός, καθώς δεν διαιρείτε από κανέναν πρώτο αριθμό μικρότερο από τη ρίζα του.

Πράγματι ισχύει $10 < \sqrt{103} < 11$ και άρα το σύνολο των πρώτων αριθμών που είναι μικρότεροι από $\sqrt{103}$ είναι $\{2, 3, 5, 7\}$.

Κανένας από τους αριθμούς 2,3,5,7 δεν διαιρεί το 103.

Θεώρημα

Υπάρχουν άπειροι πρώτοι αριθμοί

Απόδειξη

Θα αποδείξουμε το θεώρημα με απαγωγή σε άτοπο.

Απόδειξη (συνέχεια)

Ας υποθέσουμε ότι υπάρχει ένα πεπερασμένο πλήθος k από πρώτους αριθμούς και έστω $p_1, p_2, \ldots, p_k$ οι αριθμοί αυτοί.

Ο αριθμός $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$ είναι μεγαλύτερος του p_i, για κάθε i, $1 \leq i \leq k$.

Συνεπώς ο αριθμός n είναι διαφορετικός από τους $p_1, p_2, \ldots, p_k$ και άρα είναι σύνθετος αριθμός (καθώς πρώτοι αριθμοί είναι μόνο οι αριθμοί $p_1, p_2, \ldots, p_k$).

Απόδειξη (συνέχεια)

Επειδή ο n είναι σύνθετος αριθμός διαιρείται από κάποιον πρώτο αριθμό που είναι μικρότερός του.

Συνεπώς θα πρέπει $p_j \mid n$, για κάποιο j, $1 \leq j \leq k$.

Επίσης ισχύει $p_j \mid p_1 \cdot p_2 \cdot \cdots \cdot p_k$.

Επειδή ο p_j διαιρεί τους αριθμούς n και $p_1 \cdot p_2 \cdot \cdots \cdot p_k$, διαιρεί και τη διαφορά τους $n - p_1 \cdot p_2 \cdot \cdots \cdot p_k = 1$.

Απόδειξη (συνέχεια)

Άρα $p_j \mid 1$. Επειδή όμως ο μοναδικός θετικός ακέραιος που διαιρεί το 1 είναι το 1, θα πρέπει $p_j = 1$.

Αυτό είναι άτοπο, καθώς ο p_j είναι πρώτος αριθμός και άρα εξ ορισμού ισχύει $p_j > 1$.

Υποθέτοντας ότι υπάρχει πεπερασμένο πλήθος πρώτων αριθμών καταλήξαμε σε άτοπο. Άρα υπάρχουν άπειροι πρώτοι αριθμοί. □

Το παρακάτω θεώρημα, το οποίο δίνεται χωρίς απόδειξη, περιγράφει την κατανομή των πρώτων αριθμών μέσα στους θετικούς ακεραίους.

Θεώρημα

Έστω $\pi(n)$ το πλήθος των πρώτων αριθμών που είναι μικρότεροι ή ίσοι του n. Ισχύει

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

Λήμμα

Για οποιουσδήποτε θετικούς ακέραιους a, b, c, αν $gcd(a, b) = 1$ και $a \mid b \cdot c$ τότε $a \mid c$.

Απόδειξη

Έστω θετικοί ακέραιοι a, b, c, τέτοιοι ώστε $gcd(a, b) = 1$ και $a \mid b \cdot c$.

Επειδή $gcd(a, b) = 1$, από το θεώρημα του Bézout προκύπτει ότι υπάρχουν ακέραιοι s και t τέτοιοι ώστε $s \cdot a + t \cdot b = 1$.

Πολλαπλασιάζοντας τα δύο μέλη της παραπάνω ανισότητας με c προκύπτει ότι $s \cdot a \cdot c + t \cdot b \cdot c = c$.

Απόδειξη (συνέχεια)

Ισχύει $s \cdot a \cdot c = (s \cdot c) \cdot a$ και άρα $a \mid s \cdot a \cdot c$.

Επίσης έχουμε υποθέσει ότι $a \mid b \cdot c$ και άρα $a \mid t \cdot b \cdot c$.

Συνεδυάζοντας τις δύο παραπανω σχέσεις, προκύπτει ότι $a \mid s \cdot a \cdot c + t \cdot b \cdot c$.

Επειδή $s \cdot a \cdot c + t \cdot b \cdot c = c$, η παραπάνω σχέση είναι ισοδύναμη με $a \mid c$. □

Λήμμα

Έστω p ένας πρώτος αριθμός και $a_1, a_2, \ldots, a_n$ θετικοί ακέραιοι αριθμοί. Αν $p \mid \prod_{i=1}^{n} a_i$, τότε υπάρχει j, με $1 \leq j \leq n$ τέτοιο ώστε $p \mid a_j$.

Απόδειξη

Θα αποδείξουμε το θεώρημα με επαγωγή στο n.

Για $n = 1$ ισχύει $\prod_{i=1}^{n} a_i = a_1$. Συνεπώς αν $p \mid \prod_{i=1}^{n} a_i$ τότε $p \mid a_1$.

Απόδειξη (συνέχεια)

Υποθέτουμε ότι η πρόταση ισχύει για $n = k$. Θα δείξουμε ότι ισχύει και για $n = k + 1$.

Έστω ότι $p \mid \prod_{i=1}^{k+1} a_i$ που ισοδυναμεί $p \mid a_{k+1} \cdot \prod_{i=1}^{k} a_i$.

Οι μόνοι διαιρέτες του p είναι ο p και το 1. Συνεπώς $\gcd(p, a_{k+1}) \in \{1, p\}$.

Αν $\gcd(p, a_{k+1}) = p$, τότε $p \mid a_{k+1}$.

Απόδειξη (συνέχεια)

Σε αντίθετη περίπτωση έχουμε $\gcd(p, a_{k+1}) = 1$ και επίσης $p \mid a_{k+1} \cdot \prod_{i=1}^{k} a_i$.

Από το προηγούμενο λήμμα προκύπτει ότι $p \mid \prod_{i=1}^{k} a_i$.

Από την επαγωγική υπόθεση έχουμε ότι υπάρχει j τέτοιο ώστε $p \mid a_j$. □

Ορισμός

Ονομάζουμε παραγοντοποίηση ενός ακέραιου αριθμού $n > 1$ μία πεπερασμένη ακολουθία πρώτων αριθμών $p_1, p_2, \ldots, p_k$, $k \geq 1$, τέτοια ώστε $p_i \leq p_{i+1}$ για κάθε i με $1 \leq i \leq k-1$ και $\prod_{i=1}^{k} p_i = n$.

Θεώρημα

Κάθε θετικός ακέραιος αριθμός $n > 1$ έχει μία μοναδική παραγοντοποίηση.

Απόδειξη

Θα δείξουμε πρώτα με ισχυρή επαγωγή στο n, ότι κάθε $n > 1$ έχει μία παραγοντοποίηση.

Για $n = 2$, για την ακολουθία μήκους $k = 1$ με $p_1 = 2$, έχουμε $\prod_{i=1}^{k} p_i = \prod_{i=1}^{1} p_i = p_1 = 2$.

Επίσης η ιδιότητα $p_i \leq p_{i+1}$ για κάθε i με $1 \leq i \leq k - 1 = 0$ ισχύει τετριμένα, καθώς δεν υπάρχει καμία τέτοια τιμή του i.

Συνεπώς το $n = 2$ έχει μία παραγοντοποίηση.

Απόδειξη (συνέχεια)

Υποθέτουμε ότι κάθε n, με $2 \leq n \leq m$, έχει μία παραγοντοποίηση. Θα δείξουμε ότι το ίδιο ισχύει και για το $n = m + 1$.

Αν $m + 1$ είναι πρώτος αριθμός, τότε για την ακολουθία μήκους $k = 1$ με $p_1 = m + 1$, έχουμε $\prod_{i=1}^{k} p_i = \prod_{i=1}^{1} p_i = p_1 = m + 1$.

Επίσης η ιδιότητα $p_i \leq p_{i+1}$ για κάθε i με $1 \leq i \leq k - 1 = 0$ ισχύει τετριμένα.

Συνεπώς αν το $m + 1$ είναι πρώτος αριθμός, τότε έχει μία παραγοντοποίηση.

Απόδειξη (συνέχεια)

Αν $m+1$ είναι σύνθετος αριθμός, τότε υπάρχει ένας πρώτος αριθμός ο οποίος διαιρεί τον $m+1$. Έστω p ο μεγαλύτερος τέτοιος πρώτος αριθμός.

Έστω ο αριθμός $r = (m+1) \text{ div } p$. Ισχύει $m+1 = r \cdot p$, επειδή $p \mid m+1$.

Επειδή $1 < p < m+1$, θα πρέπει να ισχύει $1 < r < m+1$.

Από την επαγωγική υπόθεση προκύπτει ότι υπάρχει μία παραγοντοποίηση $p_1, p_2, \ldots, p_k$ του r. Άρα ισχύει $r = \prod_{i=1}^{k} p_i$ και $p_i \leq p_{i+1}$ για κάθε i με $1 \leq i \leq k-1$.

Απόδειξη (συνέχεια)

Αν θέσουμε $p_{k+1} = p$ έχουμε $m+1 = r \cdot p = (\prod_{i=1}^{k} p_i) \cdot p_{k+1} = \prod_{i=1}^{k+1} p_i$.

Επιπλέον επειδή $p_k \mid r$ και $r \mid m+1$, ισχύει $p_k \mid m+1$. Συνεπώς $p_k \leq p_{k+1}$, καθώς ο $p_{k+1} = p$ είναι ο μέγιστος πρώτος διαιρέτης του $m+1$.

Συνεπώς η ακολουθία $p_1, p_2, \ldots, p_k, p_{k+1}$ είναι μία παραγοντοποίηση του $m+1$.

Απόδειξη (συνέχεια)

Στη συνέχεια θα δείξουμε με απαγωγή σε άτοπο ότι για κάθε $n > 1$ δεν είναι δυνατόν να υπάρχουν δύο διαφορετικές παραγοντοποιήσεις.

Ας υποθέσουμε ότι η παραπάνω πρόταση δεν ισχύει και ας θεωρήσουμε το μικρότερο $n > 1$ για το οποίο υπάρχουν δύο παραγοντοποιήσεις $p_1, p_2, \ldots, p_k$ και $q_1, q_2, \ldots, q_\ell$.

Απόδειξη (συνέχεια)

Διακρίνουμε περιπτώσεις:

Περίπτωση 1η: $p_k = q_\ell$. Θεωρούμε τον αριθμό n div p_k και διακρίνουμε δύο υποπεριπτώσεις

Απόδειξη (συνέχεια)

Υποπερίπτωση 1α: $n \operatorname{div} p_k > 1$. Τότε ο αριθμός $n \operatorname{div} p_k$ έχει δύο παραγοντοποιήσεις $p_1, p_2, \ldots, p_{k-1}$ και $q_1, q_2, \ldots, q_{\ell-1}$.

Αυτό είναι άτοπο, επειδή ο n είναι ο μικρότερος αριθμός που είναι μεγαλύτερος του 1 και έχει δύο παραγοντοποιήσεις.

Απόδειξη (συνέχεια)

Υποπερίπτωση 1β: $n \operatorname{div} p_k = 1$. Τότε $\prod_{i=1}^{k-1} p_i = (\prod_{i=1}^{k} p_i) \operatorname{div} p_k = n \operatorname{div} p_k = 1$, που συνεπάγεται $k = 1$.

Επιπλέον $\prod_{i=1}^{\ell-1} q_i = (\prod_{i=1}^{\ell} q_i) \operatorname{div} q_\ell = n \operatorname{div} q_\ell = n \operatorname{div} p_k = 1$, που συνεπάγεται $\ell = 1$.

Συνεπώς έχουμε $k = \ell = 1$ και $p_1 = p_k = q_\ell = q_1$, που συνεπάγεται ότι οι δύο παραγοντοποιήσεις του n ταυτίζονται (άτοπο).

Απόδειξη (συνέχεια)

Περίπτωση 2η: $p_k \neq q_\ell$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $p_k > q_\ell$.

Συνεπώς $p_k > q_i$ για κάθε i, $1 \leq i \leq \ell$.

Ισχυει $n = \prod_{i=1}^{k} p_i = (\prod_{i=1}^{k-1} p_i) \cdot p_k$ και άρα $p_k \mid n$.

Επειδή $n = \prod_{i=1}^{\ell} q_i$, έχουμε ότι $p_k \mid \prod_{i=1}^{\ell} q_i$, και από το προηγούμενο λήμμα θα πρέπει να ισχύει $p_k \mid q_i$ για κάποιο i.

Το τελευταίο είναι άτοπο επειδή τα q_i είναι πρώτοι αριθμοί μικρότεροι του p_k.

Απόδειξη (συνέχεια)

Υποθέτοντας ότι υπάρχει κάποιος ακέραιος αριθμός $n > 1$ για τον οποίο υπάρχουν δύο παραγοντοποιήσεις καταλήξαμε σε άτοπο σε κάθε περίπτωση.

Συνεπώς κάθε ακέραιος αριθμός $n > 1$ έχει ακριβώς μία παραγοντοποίηση. □

Πόρισμα

Αν n είναι ένας θετικός ακέραιος αριθμός και $p_1, p_2, \ldots, p_k$ μία γνησίως αύξουσα ακολουθία πρώτων αριθμών η οποία περιέχει όλους τους πρώτους αριθμούς που διαιρούν τον n, τότε υπάρχουν μη αρνητικοί ακέραιοι $a_1, a_2, \ldots, a_k$, τέτοιοι ώστε

$$n = \prod_{i=1}^{k} p_i^{a_i}$$

Απόδειξη

Αν $n > 1$ τότε η πρόταση προκύπτει άμεσα από το προηγούμενο θεώρημα.

Επιπλέον, για $n = 1$ έχουμε $1 = \prod_{i=1}^{k} p_i^0$. □

Λήμμα

Για οποιουσδήποτε θετικούς ακέραιους αριθμούς a, c, d, αν $c \cdot d \mid c \cdot a$, τότε $d \mid a$.

Απόδειξη

Αν $c \cdot d \mid c \cdot a$, τότε υπάρχει κάποιο q τέτοιο ώστε $q \cdot c \cdot d = c \cdot a$.

Η τελευταία ισότητα συνεπάγεται $q \cdot d = a$ και άρα $d \mid a$. □

Λήμμα

Έστω q, r θετικοί ακέραιοι αριθμοί, $p_1, p_2, \ldots, p_k$ μία γνησίως αύξουσα ακολουθία πρώτων αριθμών η οποία περιέχει όλους τους πρώτους αριθμούς που διαιρούν τον q ή τον r, και έστω ότι $q = \prod_{i=1}^{k} p_i^{a_i}$ και $r = \prod_{i=1}^{k} p_i^{c_i}$, όπου $a_1, a_2, \ldots, a_k, c_1, c_2, \ldots, c_k$ είναι μη αρνητικοί ακέραιοι αριθμοί. Αν $r \mid q$, τότε για κάθε i, $1 \leq i \leq k$, ισχύει $c_i \leq a_i$.

Απόδειξη

Θα αποδείξουμε το θεώρημα με απαγωγή σε άτοπο.

Έστω ότι $r \mid q$ και ας υποθέσουμε ότι $c_j > a_j$, για κάποιο j, $1 \leq j \leq k$.

Απόδειξη (συνέχεια)

Ισχύει $p_j^{c_j} \mid r$, επειδή

$$r = \prod_{i=1}^{k} p_i^{c_i} = (\prod_{i=1}^{j-1} p_i^{c_i})(\prod_{i=j+1}^{k} p_i^{c_i}) \cdot p_j^{c_j}$$

Επειδή $r \mid q$, συμπεραίνουμε ότι $p_j^{c_j} \mid q$.

Όμως $p_j^{c_j} = p_j^{a_j} \cdot p_j^{c_j - a_j}$ και

$$q = \prod_{i=1}^{k} p_i^{a_i} = p_j^{a_j} \cdot (\prod_{i=1}^{j-1} p_i^{a_i})(\prod_{i=j+1}^{k} p_i^{a_i})$$

Απόδειξη (συνέχεια)

Άρα έχουμε

$$p_j^{a_j} \cdot p_j^{c_j - a_j} \mid p_j^{a_j} \cdot (\prod_{i=1}^{j-1} p_i^{a_i})(\prod_{i=j+1}^{k} p_i^{a_i})$$

που από το προηγούμενο λήμμα συνεπάγεται

$$p_j^{c_j - a_j} \mid \cdot (\prod_{i=1}^{j-1} p_i^{a_i})(\prod_{i=j+1}^{k} p_i^{a_i})$$

Απόδειξη (συνέχεια)

Επειδή $c_j > a_j$, ισχύει $p_j \mid p_j^{c_j - a_j}$.

Συνδυάζοντας τις δύο τελευταίες σχέσεις προκύπτει ότι

$$p_j \mid (\prod_{i=1}^{j-1} p_i^{a_i})(\prod_{i=j+1}^{k} p_i^{a_i})$$

Η τελευταία πρόταση όμως συνεπάγεται ότι $p_j \mid p_i$, για κάποιο $i \neq j$, το οποίο είναι άτοπο.

Απόδειξη (συνέχεια)

Υποθέτοντας ότι $c_j > a_j$, για κάποιο j, $1 \leq j \leq k$, καταλήξαμε σε άτοπο. Άρα για κάθε i, $1 \leq i \leq k$, ισχύει $c_i \leq a_i$. □

Θεώρημα

Έστω m, n θετικοί ακέραιοι αριθμοί και $p_1, p_2, \ldots, p_k$ όλοι οι πρώτοι αριθμοί που είναι μικρότεροι ή ίσοι από το $\max(m, n)$. Αν $m = \prod_{i=1}^{k} p_i^{a_i}$ και $n = \prod_{i=1}^{k} p_i^{b_i}$, όπου $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$ είναι μη αρνητικοί ακέραιοι αριθμοί, τότε $\gcd(m, n) = \prod_{i=1}^{k} p_i^{\min(a_i, b_i)}$.

Απόδειξη

Έστω $d = \prod_{i=1}^{k} p_i^{\min(a_i, b_i)}$.

Δείχνουμε πρώτα ότι $d \mid m$ και $d \mid n$.

Απόδειξη (συνέχεια)

Ισχύει $p_i^{a_i} = p_i^{a_i - \min(a_i,b_i)} \cdot p_i^{\min(a_i,b_i)}$

Συνεπώς

$$\begin{aligned} m &= \prod_{i=1}^{k} p_i^{a_i} = \prod_{i=1}^{k} (p_i^{a_i - \min(a_i,b_i)} \cdot p_i^{\min(a_i,b_i)}) \\ &= (\prod_{i=1}^{k} p_i^{a_i - \min(a_i,b_i)}) \cdot (\prod_{i=1}^{k} p_i^{\min(a_i,b_i)}) \\ &= (\prod_{i=1}^{k} p_i^{a_i - \min(a_i,b_i)}) \cdot d \end{aligned}$$

Άρα $d \mid m$. Με ανάλογο τρόπο προκύπτει ότι $d \mid n$.

Απόδειξη (συνέχεια)

Απομένει να δείξουμε ότι ο d είναι μεγαλύτερος ή ίσος από οποιονδήποτε κοινό διαιρέτη των m και n.

Έστω r ένας θετικός ακέραιος τέτοιος ώστε $r \mid m$ και $r \mid n$.

Τότε $r \leq \max(m, n)$ και άρα όλοι οι πρώτοι διαιρέτες του r είναι ανάμεσα στους $p_1, p_2, \ldots, p_k$.

Συνεπώς $r = \prod_{i=1}^{k} p_i^{c_i}$, όπου $c_1, c_2, \ldots, c_k$ είναι μη αρνητικοί ακέραιοι αριθμοί.

Απόδειξη (συνέχεια)

Επειδή $r \mid m$, ισχύει $c_i \leq a_i$ για κάθε i, $1 \leq i \leq k$.

Ομοίως, επειδή $r \mid n$, ισχύει $c_i \leq b_i$ για κάθε i, $1 \leq i \leq k$.

Από τα παραπάνω προκύπτει ότι $c_i \leq \min(a_i, b_i)$ για κάθε i, $1 \leq i \leq k$.

Συνεπώς

$$r = \prod_{i=1}^{k} p_i^{c_i} \leq \prod_{i=1}^{k} p_i^{\min(a_i, b_i)} = d$$

Απόδειξη (συνέχεια)

Δείξαμε ότι ο d διαιρεί τους m και n και για κάθε κοινό διαιρετη r των m και n ισχύει $r \leq d$.

Συνεπώς $d = \gcd(m, n)$. □

Ελάχιστο Κοινό Πολλαπλάσιο

Ορισμός

Έστω δύο θετικοί ακέραιοι αριθμοί a και b. Ονομάζουμε ελάχιστο κοινό πολλαπλάσιο τον αριθμό $\text{lcm}(a, b) = \min\{m > 0 \in \mathbb{Z} : a \mid m \text{ και } b \mid m\}$.

Θεώρημα

Έστω m, n θετικοί ακέραιοι αριθμοί και $p_1, p_2, \ldots, p_k$ όλοι οι πρώτοι αριθμοί που είναι μικρότεροι ή ίσοι από το $m \cdot n$. Αν $m = \prod_{i=1}^{k} p_i^{a_i}$ και $n = \prod_{i=1}^{k} p_i^{b_i}$, όπου $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$ είναι μη αρνητικοί ακέραιοι αριθμοί, τότε $\operatorname{lcm}(m, n) = \prod_{i=1}^{k} p_i^{\max(a_i, b_i)}$.

Απόδειξη

Έστω $q = \prod_{i=1}^{k} p_i^{\max(a_i, b_i)}$.

Δείχνουμε πρώτα ότι $m \mid q$ και $n \mid q$.

Απόδειξη (συνέχεια)

Ισχύει $p_i^{\max(a_i,b_i)} = p_i^{\max(a_i,b_i)-a_i} \cdot p_i^{a_i}$

Συνεπώς

$$\begin{aligned} q &= \prod_{i=1}^{k} p_i^{\max(a_i,b_i)} = \prod_{i=1}^{k} (p_i^{\max(a_i,b_i)-a_i} \cdot p_i^{a_i}) \\ &= (\prod_{i=1}^{k} p_i^{\max(a_i,b_i)-a_i}) \cdot (\prod_{i=1}^{k} p_i^{a_i}) \\ &= (\prod_{i=1}^{k} p_i^{\max(a_i,b_i)-a_i}) \cdot m \end{aligned}$$

Άρα $m \mid q$. Με ανάλογο τρόπο προκύπτει ότι $n \mid q$.

Απόδειξη (συνέχεια)

Απομένει να δείξουμε ότι ο q είναι μικρότερος ή ίσος από οποιοδήποτε κοινό πολλαπλάσιο των m και n.

Δείχνουμε πρώτα ότι $q \leq m \cdot n$:

$$\begin{aligned} q &= \prod_{i=1}^{k} p_i^{\max(a_i,b_i)} \leq \prod_{i=1}^{k} p_i^{a_i+b_i} = \prod_{i=1}^{k} (p_i^{a_i} \cdot p_i^{b_i}) \\ &= (\prod_{i=1}^{k} p_i^{a_i}) \cdot (\prod_{i=1}^{k} p_i^{b_i}) = m \cdot n \end{aligned}$$

Απόδειξη (συνέχεια)

Έστω s ένας θετικός ακέραιος τέτοιος ώστε $m \mid s$ και $n \mid s$.

Αν $s > m \cdot n$, τότε από την προηγούμενη ανισότητα προκύπτει ότι $q < s$.

Αν $s \leq m \cdot n$, τότε όλοι οι πρώτοι διαιρέτες του s είναι ανάμεσα στους $p_1, p_2, \ldots, p_k$.

Συνεπώς $s = \prod_{i=1}^{k} p_i^{c_i}$, όπου $c_1, c_2, \ldots, c_k$ είναι μη αρνητικοί ακέραιοι αριθμοί.

Απόδειξη (συνέχεια)

Επειδή $m \mid s$, ισχύει $a_i \leq c_i$ για κάθε i, $1 \leq i \leq k$.

Ομοίως, επειδή $n \mid s$, ισχύει $b_i \leq c_i$ για κάθε i, $1 \leq i \leq k$.

Από τα παραπάνω προκύπτει ότι $\max(a_i, b_i) \leq c_i$ για κάθε i, $1 \leq i \leq k$.

Συνεπώς

$$q = \prod_{i=1}^{k} p_i^{\max(a_i, b_i)} \leq \prod_{i=1}^{k} p_i^{c_i} = s$$

Απόδειξη (συνέχεια)

Δείξαμε ότι ο q είναι πολλαπλάσιο των m και n και για κάθε κοινό πολλαπλάσιο s των m και n ισχύει $q \leq s$.

Συνεπώς $q = \mathrm{lcm}(m, n)$. □

Τα παρακάτω θεώρημα περιγράφει τη σχέση ανάμεσα στο ελάχιστο κοινό πολλαπλάσιο και στο μέγιστο κοινό διαιρέτη δύο θετικών αριθμών, η οποία μπορεί να χρησιμοποιηθεί για τον υπολογισμό του ελάχιστου κοινού πολλαπλάσιου.

Θεώρημα

Για οποιουσδήποτε θετικούς ακέραιους αριθμούς m, n ισχύει $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = m \cdot n$.

Απόδειξη

Παρατηρούμε ότι για οποιουσδήποτε ακέραιους a, b ισχύει $\min(a, b) + \max(a, b) = a + b$.

Απόδειξη (συνέχεια)

$$
\begin{aligned}
\gcd(m,n)\cdot \operatorname{lcm}(m,n) &= \Big(\prod_{i=1}^{k} p_i^{\min(a_i,b_i)}\Big)\cdot\Big(\prod_{i=1}^{k} p_i^{\max(a_i,b_i)}\Big)\\
&= \prod_{i=1}^{k}\big(p_i^{\min(a_i,b_i)}\cdot p_i^{\max(a_i,b_i)}\big)\\
&= \prod_{i=1}^{k} p_i^{\min(a_i,b_i)+\max(a_i,b_i)}\\
&= \prod_{i=1}^{k} p_i^{a_i+b_i}\\
&= \prod_{i=1}^{k}\big(p_i^{a_i}\cdot p_i^{b_i}\big)\\
&= \Big(\prod_{i=1}^{k} p_i^{a_i}\Big)\cdot\Big(\prod_{i=1}^{k} p_i^{b_i}\Big)\\
&= m\cdot n
\end{aligned}
$$