Θεωρία Αριθμών VI

Πρώτοι Αριθμοί
(Prime Numbers)

Βαγγέλης Ψύχας

Πρώτοι Αριθμοί

✧ Ένας ακέραιος αριθμός $p \neq 0, \pm 1$ θα λέγεται **πρώτος αριθμός** ή απλά **πρώτος** αν οι μόνοι θετικοί διαιρέτες του είναι το 1 και ο $|p|$.

✧ Ένας ακέραιος $a \neq \pm 1$ που δεν είναι πρώτος θα λέγεται **σύνθετος**.

✧ Κάθε σύνθετος ακέραιος $a \neq \pm 1$ μπορεί να γραφεί σαν γινόμενο δύο ακεραίων διαφορετικών από το ± 1 .

Πρώτοι Αριθμοί

✧ Οι αριθμοί 1 και -1 δεν χαρακτηρίζονται ούτε πρώτοι ούτε σύνθετοι.

✧ Κάθε πρώτος p που διαιρεί τον ακέραιο a, θα λέγεται πρώτος διαιρέτης του a.

✧ Είναι προφανές ότι ισχύει η ισοδυναμία: $-p$ πρώτος $\Leftrightarrow$ p πρώτος.
(γι' αυτό περιοριζόμαστε μόνο σε θετικούς πρώτους)

Πρώτοι Αριθμοί

- Κάθε ακέραιος μεγαλύτερος του 1 έχει ένα τουλάχιστον πρώτο διαιρέτη.

- Αν a είναι σύνθετος ακέραιος μεγαλύτερος του 1, τότε υπάρχει ένας τουλάχιστον πρώτος αριθμός p, τέτοιος ώστε $p|a$ και $p < \sqrt{a}$.

- Υπάρχουν άπειροι θετικοί πρώτοι ακέραιοι.

Πρώτοι Αριθμοί

♦ Αν ένας πρώτος αριθμός p διαιρεί το γινόμενο ab δύο ακεραίων, τότε θα διαιρεί έναν τουλάχιστον από αυτούς τους ακεραίους.

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

Πρώτοι Αριθμοί

- Κάθε θετικός ακέραιος $a > 1$ μπορεί να γραφεί κατά μοναδικό τρόπο στη μορφή

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$$

όπου οι $p_1, p_2, \cdots, p_k$ είναι θετικοί πρώτοι με $p_1 < p_2 < \cdots < p_k$ και $a_1, a_2, \cdots, a_k$ θετικοί ακέραιοι.

- Η μορφή $a = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$ ονομάζεται **κανονική μορφή** του θετικού ακέραιου a.

Πρώτοι Αριθμοί

✧ Ο **μκδ** θετικών ακέραιων που είναι γραμμένοι σε κανονική μορφή είναι ίσος με το γινόμενο των κοινών τους παραγόντων και με τον κάθε παράγοντα υψωμένο στον μικρότερο εμφανιζόμενο εκθέτη.

✧ Π.χ αν $a = 2^3 \cdot 3 \cdot 5^3$ και $b = 2^2 \cdot 3^4$ τότε:

$$(a, b) = 2^2 \cdot 3$$

Πρώτοι Αριθμοί

✧ Το **εκπ** θετικών ακέραιων που είναι γραμμένοι σε κανονική μορφή είναι ίσος με το γινόμενο των κοινών και μη κοινών παραγόντων και με τον κάθε παράγοντα υψωμένο στο μεγαλύτερο εμφανιζόμενο εκθέτη.

✧ Π.χ αν $a = 2^3 \cdot 3 \cdot 5^3$ και $b = 2^2 \cdot 3^4$ τότε:

$$[a, b] = 2^3 \cdot 3^4 \cdot 5^3$$

Πρώτοι Αριθμοί

✧ Αν ο αριθμός $a = 2^n - 1, n \in \mathbb{N}^*$ είναι πρώτος, να αποδείξετε ότι και ο αριθμός n είναι πρώτος.

✧ Έστω ότι ο αριθμός $a = 2^n - 1, n \in \mathbb{N}^*$ είναι πρώτος και ας υποθέσουμε (για να καταλήξουμε σε άτοπο) ότι ο αριθμός n δεν είναι πρώτος. Τότε $n = k \cdot l$ (όπου k, l ακέραιοι μεγαλύτεροι του 1). Άρα $a = 2^n - 1 = 2^{k \cdot l} - 1 =$

$$= \left(2^k\right)^l - 1 = \left(2^k - 1\right)\left(\left(2^k\right)^{l-1} + \left(2^k\right)^{l-2} + \cdots + 1\right).$$

Άρα ο αριθμός $2^k - 1$ είναι παράγοντας του αριθμού $a = 2^n - 1$ με $1 < 2^k - 1 < 2^n - 1$. Δηλαδή ο αριθμός $a = 2^n - 1$ είναι σύνθετος (άτοπο).

Πρώτοι Αριθμοί

✧ Αποδείξτε ότι ο $\sqrt{2}$ είναι άρρητος.

✧ Έστω (για να καταλήξουμε σε άτοπο) ότι ο $\sqrt{2}$ είναι ρητός.
Τότε θα υπάρχουν θετικοί ακέραιοι m, n (πρώτοι μεταξύ τους)
ώστε: $\sqrt{2} = \frac{m}{n}$.

Τότε $m = \sqrt{2} \cdot n \Rightarrow m^2 = 2n^2 \Rightarrow (m^2$ άρτιος$) \Rightarrow (m$ άρτιος$) \Rightarrow$
$\Rightarrow m = 2k$. Άρα $4k^2 = 2n^2 \Rightarrow n^2 = 2k^2 \Rightarrow$
$\Rightarrow (n^2$ άρτιος$) \Rightarrow (n$ άρτιος$)$,
άτοπο (διότι m, n πρώτοι μεταξύ τους).

Πρώτοι Αριθμοί

✧ Αν ο φυσικός αριθμός n δεν είναι τετράγωνο φυσικού, να αποδειχτεί ότι ο $\sqrt{n}$ είναι άρρητος.

✧ Έστω (για να καταλήξουμε σε άτοπο) ότι ο $\sqrt{n}$ είναι ρητός.
Τότε θα υπάρχουν θετικοί ακέραιοι k, m (πρώτοι μεταξύ τους)

ώστε: $\sqrt{n} = \frac{k}{m}$.

Τότε $k = \sqrt{n} \cdot m \Rightarrow k^2 = n \cdot m^2$. Αν $m = 1$ τότε $k^2 = n$ (άτοπο διότι ο n δεν είναι τετράγωνο ακεραίου)

Άρα $m > 1$ και κατά συνέπεια ο m θα έχει ένα πρώτο διαιρέτη p.

Δηλαδή $p|k^2 \Rightarrow p|k$ και επειδή $p|m$ καταλήγουμε $p|(k, m)$

(άτοπο διότι οι αριθμοί ακέραιοι k, m είναι πρώτοι μεταξύ τους).

Πρώτοι Αριθμοί

✧ Υπάρχουν n διαδοχικοί ακέραιοι (n θετικός ακέραιος) που δεν είναι πρώτοι.

✧ Θεωρούμε του ακέραιους:

$$m_1 = (n+1)! + 2, m_2 = (n+1)! + 3, \cdots, m_n = (n+1) + n + 1.$$

Τότε οι αριθμοί $m_i, i = 1, 2, 3, \cdots, n$ είναι διαδοχικοί και

$$(i+1) | m_i, i = 1, 2, 3, \cdots, n.$$

Πρώτοι Αριθμοί

✧ Αν ο p είναι πρώτος, τότε κάθε αριθμός m θα είναι είτε πολλαπλάσιο του p είτε σχετικά πρώτος με τον p.
Δηλαδή: $(m = k \cdot p$ ή $(m, p) = 1)$.

✧ Έστω $(m, p) = d$ τότε $d|p$ και επειδή ο p είναι πρώτος, θα ισχύει $d = 1$ ή $d = p$. Δηλαδή $(m, p) = 1$ ή $(m, p) = p$.
Από την πρώτη ισότητα συμπεραίνουμε ότι ο m είναι σχετικά πρώτος με τον p και από τη δεύτερη ότι ο p διαιρεί τον m.

Πρώτοι Αριθμοί

✧ Αν ο p είναι πρώτος και διαιρεί το γινόμενο κάποιων αριθμών, τότε θα διαιρεί έναν τουλάχιστον από αυτούς τους αριθμούς.

✧ Έστω ότι $p|m_1 \cdot m_2 \cdot \cdots \cdot m_k$.

Αν ο p δεν διαιρεί τον m_1 τότε θα είναι πρώτος με αυτόν, οπότε $p|m_2 \cdot \cdots \cdot m_k$.

Αν ο p δεν διαιρεί τον m_2 τότε θα είναι πρώτος με αυτόν, οπότε $p|m_3 \cdot \cdots \cdot m_k$. …

Αν ο p δεν διαιρεί τον m_{k-1} τότε θα είναι πρώτος με αυτόν, οπότε $p|m_k$.

Δίδυμοι Πρώτοι

✧ Δύο πρώτοι θα λέγονται **δίδυμοι** όταν διαφέρουν κατά δύο.

✧ Παραδείγματα δίδυμων πρώτων:

$3, 5 \quad 5, 7 \quad 11, 13 \quad 17, 19 \quad 29, 31 \quad 41, 43$

✧ Το μεγαλύτερο ζεύγος δίδυμων πρώτων που έχει βρεθεί είναι το: $3756801695685 \cdot 2^{666669} \pm 1$.
(200700 ψηφία)

✧ Το γενικότερο πρόβλημα δεν έχει λυθεί.