22/10/2018

· Ευκλείδεια Διαίρεση

Πρόταση: Έστω $a, b \in \mathbb{Z}$ με $b \neq 0$. Τότε υπάρχουν μοναδικά $q, r \in \mathbb{Z}$ ώστε $a = q \cdot b + r$ και $0 \leq r < |b|$.

Το q λέγεται πηλίκο της διαίρεσης του a με το b.

Το r λέγεται υπόλοιπο της διαίρεσης του a με το b.

Παραδείγματα

$a = 30,\ b = 2 \rightarrow q = 15,\ r = 0$

$a = -30,\ b = 2 \rightarrow q = -15,\ r = 0$

$a = 31,\ b = 2 \rightarrow q = 15,\ r = 1$

$a = 30,\ b = -2 \rightarrow q = -15,\ r = 0$

$a = 31,\ b = -2 \rightarrow q = -15,\ r = 1$

προσοχή! $a = -31,\ b = 2 \rightarrow q = -16,\ r = 1$.

Προσοχή: Πρέπει $0 \leq r \leq |b| - 1$

Απόδειξη Πρότασης:

Ισχυρισμός - 1: Έστω αι $q, q', r, r' \in \mathbb{Z}$ με

(1) $a = q \cdot b + r = q' \cdot b + r'$ και $0 \leq r \leq |b|$

και $0 \leq r' < |b|$

Υποθέταμε $r \neq r'$ και θα βρούμε αντίφαση.

Αφού $r \neq r'$ έχουμε $q \neq q'$. Η (1) δίνει $q \cdot b + r = q'b + r' \Rightarrow$

$b(q - q') = r' - r$

$\Rightarrow |b(q - q')| = |r - r'| = |b||q - q'| = |r - r'|$ (2)

Αφού $q, q' \in \mathbb{Z}$ με $q \neq q' \Rightarrow |q - q'| \geq 1$

Άρα η (2) $\Rightarrow$: $|r - r'| \geq |b|$

Αλλά $\left.\begin{array}{l} 0 \le r < |b| \\ 0 \le r' < |b| \\ r \ne r' \end{array}\right\} \Rightarrow |r' - r| < |b|$ αντίφαση

Ύπαρξη q, r

Θέτουμε $A = \{ k \in \mathbb{Z}_{\ge}$ με τις ιδιότητες $k \ge 0$, και υπάρχει $l \in \mathbb{Z}$ ώστε $k = a - lb \}$

Ισχυρισμός - 1: $A \ne \emptyset$

Απόδειξη:

Αν $b > 0$, θέτουμε l αρνητικό και με μεγάλη απόλυτο τιμή.

Αν $b < 0$, θέτουμε l θετικό πολύ μεγάλο.

Αφού A μη κενό φραγμένο κάτω υποσύνολο του $\mathbb{Z}$ από θεώρημα το A έχει ελάχιστο στοιχείο, έστω r.

Συνεπώς, υπάρχει $q \in \mathbb{Z}$ με $r = a - qb \Rightarrow a = qb + r$

Ισχυρισμός: $0 \le r < |b|$.

Απόδειξη:

Περίπτωση 1: $b > 0$ Αν $r \ge b$ τότε και $r - 1 \in A$ αντίφαση

Παρόμοια όταν $b < 0$.

Παρατήρηση: Η απόδειξη μας λέει ότι το υπόλοιπο r της διαίρεσης του a με το b είναι ο ελάχιστος μη αρνητικός ακέραιος που γράφεται στη μορφή $a - lb$ για $l \in \mathbb{Z}$.

Ερώτημα: Δοθέντων $a, b \in \mathbb{Z}$ με $b \ne 0$ πως υπολογίζουμε τα q και r, Αλγόριθμος Υπολογισμού q, r.

Περιπτ. 1: $a \geq 0$, $b > 0$.

Εκτελούμε τη διαίρεση που ξέρουμε από το Δημοτικό.

Παράδειγμα.

$a = 123$, $b = 11$

$$\begin{array}{r|l} 123 & 11 \\ -11 & 11 \\ \hline 13 & \\ -11 & \\ \hline 2 & \end{array}$$

Περίπτωση 2: $a < 0$, $b > 0$

Βήμα 1: Κάνουμε διαίρεση του $|a| = -a > 0$ με το b και έστω $|a| = q_1 b + r_1$ με $0 \leq r_1 < b$.

Βήμα 2: Αν $r_1 = 0$, τότε $q = -q_1$, $r = 0$

Αν $r_1 > 0$, θέτουμε $q = -q_1 - 1$, $r = b - r_1$

Παράδειγμα 1: $a = -20$, $b = 2$

Τότε $|a| = 20 = 2 \cdot 10 + 0$ άρα $a = -20 = (-10) \cdot 2 + 0$

και $q_1 = 10$, $r_1 = 0$, $q = -q_1 = -10$, $r = 0$

Παράδειγμα 2: $a = -21$, $b = 2$

$\Rightarrow |a| = 21 = 2 \cdot 10 + 1$, άρα $q_1 = 10$, $r_1 = 1$

Θέτουμε $q = -10 - 1 = -11$ και $r = 2 - 1 = 1$

Πράγματι, $(-11) \cdot 2 + 1 = -21 = a$

Περίπτωση $b < 0$.