25/10/2018

Υπενθύμιση: Αν $a, b \in \mathbb{Z}$ με $b \neq 0$, τότε υπάρχουν μοναδικά $q, r \in \mathbb{Z}$ ώστε $a = qb + r$ και $0 \le r < |b|$

πηλίκο (q) υπόλοιπο (r)

ΑΛΓΟΡΙΘΜΟΣ ΥΠΟΛΟΓΙΣΜΟΥ q, r

Περίπτωση-1: $a \ge 0$, $b < 0$

Περίπτωση-2: $a < 0$, $b > 0$

Περίπτωση-3: $b < 0$

Έστω $b<0$ κάνουμε Ευκλείδεια Διαίρεση του a με το $|b|$. Έστω q_1 το πηλίκο και r_1 το υπόλοιπο της Ευκλείδειας Διαίρεσης του a με το $|b|$. Τότε $q = -q_1$, $r = r_1$, δηλ. το πηλίκο της Ευκλ. Διαίρεσης του a με το b είναι $-q_1$ και το υπόλοιπο r_1.

(Απόδειξη: $a = q_1|b| + r_1 \Rightarrow a = q_1(-b) + r_1 = (-q_1)b + r_1$

Φυλλάδιο 3 / Άσκηση 5

Βρείτε q, r όταν

a) $a = 352$ $b = 7$

$$\begin{array}{r|l} 352 & 7 \\ \hline 2 & 50 \end{array}$$

$q = 50$, $r = 2$

c) $a = -352$, $b = 7$.

Κάνουμε διαίρεση $|a| = 352$ με το 7, έχω πηλίκο $q_1 = 50$, υπόλοιπο $r_1 = 2$. Αφού $r_1 \neq 0$ έχουμε $q = -q_1 - 1 = -51$, $r = b - r_1 = 7 - 2 = 5$

(Πράγματι $(-51)\cdot 7 + 5 = \cancel{-375}\ -357 + 5 = a$.)

b) $a=352$ $b=-7$

Η ευκλείδεια διαίρεση του α με το $|b|$ έχει $q_1=50$, $r_1=2$

Άρα $q=-q_1=-50$, $r=r_1=2$

(Επαλ. $(-50)(-7)+2=a$)

d) $a=-357$, $b=-7$

Η ευκλείδεια διαίρεση του α με το $|b|$ από το c έχει $q_1=-51$, $r_1=5$. Άρα $q=-q_1=51$, $r=r_1=5$

(Επαλ. $51\cdot(-7)+5=-357+5=a$.)

· Ν-αδικό ανάπτυγμα ακεραίου.

Συμβολισμός: Έστω $n\geq 2$ ακέραιος, $r\geq 0$ ακέραιος και $a_0, a_1 \dots a_r$ ακέραιοι με $0\leq a_i\leq n-1$ για κάθε i

Θέτουμε $(a_r, a_{r-1}, \dots, a_1, a_0)_n = a_0 + a_1 n + a_2 n^2 + a_3 n^3 + \dots + a_r n^r \in \mathbb{Z}$

Πχ $(3,0,7)_{10} = 7+0\cdot 10+3\cdot 10^2=307$

$(1,0,1,1)_2 = 1+1\cdot 2^1+0\cdot 2^2+1\cdot 2^3 = 11$

Θεώρημα:

Έστω $n\geq 2$ ακέραιος, και $k\in\mathbb{Z}$ με $k>0$. Τότε υπάρχουν μοναδικά $r\geq 0$ και $a_0,\dots,a_r\in\mathbb{Z}$ με $0\leq a_i\leq n-1$ για κάθε i και $a_r\neq 0$ ώστε $k=(a_r, a_{r-1}, \dots, a_1, a_0)_n$.

Η παραπάνω έκφραση λέγεται n-δικό ανάπτυγμα του k.

Απόδειξη:
Ύπαρξη: θα δώσουμε αλγόριθμο
Μοναδικότητα: Προκύπτει από μοναδικότητα πηλίκου και υπολοίπου στην ευκλείδεια διαίρεση.

ΑΛΓΟΡΙΘΜΟΣ: Έστω $n \geq 2$ και $k > 0$ ακέραιοι.

Βήμα-1: Υπολογίζουμε το (μοναδικό) r ώστε $n^r \leq k \leq n^{r+1}$
Εκτελούμε ευκλ. διαίρεση του k με το n^r. Συμβολίζουμε a_r το πηλίκο της διαίρεσης b_r το υπόλοιπο της διαίρεσης,

$k = a_r n^r + \dots + a_1 n + a_0$
με $0 \leq a_i \leq n-1$ $\forall i$ και $a_r \neq 0$

Βήμα-2: Θέτουμε $k' = k - a_r n^r$ και εφαρμόζουμε Βήμα-1 για το $k' < k$.

Παράδειγμα
Βρείτε το 3-δικό ανάπτυγμα του 29.

ΛΥΣΗ
Βήμα-1: Υπολογίζουμε το r με $3^r \leq 29 < 3^{r+1}$
Άρα $r = 3$. Εκτελούμε ευκλ. διαίρεση του 29 με το $3^3 = 27$.
Έχουμε $29 = 1 \cdot 3^3 + 2$. Άρα $a_3 = 1$. Δηλ. το ανάπτυγμα της μορφής $(1, a_2, a_1, a_0)_3$.

Βήμα-2: Θέτουμε $k' = 29 - 1 \cdot 3^3 = 2$ που έχει ανάπτυγμα $(2)_3$.
Συνεπώς $29 = (1,0,0,2)_3$.

Ορισμός: Έστω $n=10$ και $n \geq 1$ με 10-δικό ανάπτυγμα $n=(a_r, a_{r-1}, \ldots, a_1, a_0)_{10}$. Τότε τα a_i λέγονται δεκαδικά ψηφία του n και το a_0 τελευταίο δεκαδικό ψηφίο.

Παράδειγμα: $30578 = (3,0,5,7,8)_{10}$

• Μέγιστος Κοινός Διαιρέτης •

Ορισμός: Έστω $a, b \in \mathbb{Z}$. Λέμε ότι ο a διαιρεί το b, και γράφουμε $a|b$ όταν υπάρχει $k \in \mathbb{Z}$ με $b = ka$

Παράδειγμα: $2|8$ γιατί $8 = 4 \cdot 2$

Αλγόριθμος: Έστω $a, b \in \mathbb{Z}$ με $b \neq 0$ και r το υπόλοιπο της ευκλ. διαίρεσης του a με το b. Τότε $b|a$ αν-ν $r=0$.

Παράδειγμα: 7 δεν διαιρεί το 352 γιατί όπως είδαμε το υπόλοιπο r της ευκλ. διαιρ. του 352 με το 7 είναι 2.

Παρατήρηση:
Ο λόγος που δουλεύει ο Αλγόριθμος είναι η μοναδικότητα του υπολοίπου r στην Ευκλ. Διαίρεση.

Πρόταση:
Έστω $a, b \in \mathbb{Z}$ με $b|a$ και $a \neq 0$. Τότε $|b| \leq |a|$.

Απόδειξη

Αφού $b|a$ υπάρχει $k \in \mathbb{Z}$ με $a = kb$ (1). Αφού $a \neq 0 \Rightarrow k \neq 0$.
Η (1) $\Rightarrow |a| = |k||b|$ (2). Αφού $k \in \mathbb{Z}$ με $k \neq 0$, έπεται $|k| \geq 1$.
Συνεπώς (2) $\Rightarrow |b| \leq |a|$

Παρατήρηση

Στα επόμενα θα γράφουμε $(a,b) \neq (0,0)$. Αυτό σημαίνει ότι τουλάχιστον ένα από τα a, b ΔΕΝ είναι μηδέν.

Ορισμός

Έστω $a, b \in \mathbb{Z}$ με $(a,b) \neq (0,0)$. Θέτουμε $S = \{k \in \mathbb{N} : k|a$ και $k|b\}$. Το $S \neq \emptyset$, γιατί $1 \in S$. Από την πρόταση το S είναι άνω φραγμένο.
Από θεώρημα το S έχει (μοναδικό) μέγιστο στοιχείο, το οποίο ονομάζουμε Μέγιστο Κοινό Διαιρέτη (Μ.Κ.Δ) των a, b και συμβολίζουμε Μ.Κ.Δ.(a,b) (και στη θεωρία αριθμών (a,b)).

Παράδειγμα.

Αν $a=4$, $b=6$, $S = \{1, 2\}$ και ΜΚΔ$(a,b) = 2$.

Πρόταση: Έστω $a, b, d, x, y \in \mathbb{Z}$. Αν $d|a$ και $d|b$ τότε $d | xa + yb$.

Απόδειξη

Αφού $d|a$ υπάρχει $k_1 \in \mathbb{Z}$ με $a = k_1 \cdot d$.
Αφού $d|b$ υπάρχει $k_2 \in \mathbb{Z}$ με $b = k_2 \cdot d$.
Τότε $xa + yb = xk_1 d + yk_2 \cdot d = d(xk_1 + yk_2) \Rightarrow d | (xa + yb)$.

Παράδειγμα

$d|2018$ και $d|2020 \Rightarrow d | (1 \cdot 2020 + (-1) \cdot 2018) \Rightarrow d|2$

Παρατήρηση

Έστω $a, b \in \mathbb{Z}$ όχι και τα δύο μηδέν και $k \in \mathbb{Z}$. Τότε ένας τουλάχιστον από τους $a-kb, b$ είναι μη μηδενικός

Απόδειξη

Αν $\left.\begin{array}{l} a-kb=0 \\ b=0 \end{array}\right\} \Rightarrow a-b=0$ αντίφαση.

Πρόταση

Έστω $a, b \in \mathbb{Z}$ όχι και τα δύο μηδέν και $k \in \mathbb{Z}$.
Τότε $\text{ΜΚΔ}(a,b) = \text{ΜΚΔ}(a-kb, b)$.

Απόδειξη

Θέτουμε $d_1 = \text{ΜΚΔ}(a,b)$, $d_2 = \text{ΜΚΔ}(a-kb, b)$
Θα δείξουμε ότι $d_1 = d_2$, δείχνουμε ότι $d_1 \leq d_2$ και $d_2 \leq d_1$

Έχουμε $\left\{\begin{array}{l} d_1 | a \overset{\text{πρ}}{\Rightarrow} d_1 | a-kb \\ d_1 | b \Rightarrow d_1 | b \end{array}\right. \Rightarrow d_1 \leq d_2$, γιατί;

$d_2 = \text{ΜΚΔ}(a-kb, b)$

Έχουμε $\left.\begin{array}{l} d_2 | a-kb \\ d_2 | b \end{array}\right\} \overset{\text{πρ}}{\Rightarrow} \left\{\begin{array}{l} d_2 | (a-kb)+kb \\ d_2 | b \end{array}\right. \Rightarrow \left\{\begin{array}{l} d_2 | a \\ d_2 | b \end{array}\right. \Rightarrow d_2 \leq d_1$.

Παρατηρήσεις.

- Έστω $a \neq 0$ και $b = 0$. Τότε $ΜΚΔ(a,b) = ΜΚΔ(a,0) = |a|$ γιατί κάθε ακέραιος διαιρεί το 0, και ο μέγιστος διαιρέτης του a είναι η $|a|$.

  Παράδ. $ΜΚΔ(-2018, 0) = 2018$.

- Έστω $a \in \mathbb{Z}$. Τότε οι ακέραιοι a και $-a$ έχουν το ίδιο σύνολο διαιρετών γιατί αν $d|a \Rightarrow$ υπάρχει $k \in \mathbb{Z}$ με $a = kd \Rightarrow -a = (-k)d$ και αντίστροφα. Άρα αν $a, b \in \mathbb{Z}$ έχει και τα δύο μηδέν.

  Το σύνολο των θετικών κοινών διαιρετών των a, b είναι ίσο με το σύνολο των θετικών κοινών διαιρετών των $|a|, |b|$. Άρα
  $ΜΚΔ(a,b) = ΜΚΔ(|a|, |b|)$.