

Author:

Title: Γεννήτορες τύποι κριτηρίων διαιρετότητας. Σχέση ισοτιμίας  
(Mod2)–ΥΠ:( $a \cdot x^3 + \delta$ )

Creator: HDML

## Γεννήτορες τύποι κριτηρίων διαιρετότητας Σχέση Ισοτιμίας (mod δ) – ΥΠ: $\left(\frac{a}{[x]}, \delta\right)$

Νικ. Δ. Ψαθάς

Κάθε φυσικός αριθμός με  $(v + 1)$  ψηφία γράφεται  $\frac{a}{[x]} = \overline{a_0 a_1 a_2 \dots a_v}$   
 $= a_0 x^v + a_1 x^{v-1} + a_2 x^{v-2} + \dots + a_{v-1} x + a_v$  όπου  $x$  η βάση του συστήματος  
αρίθμησης και  $a_0, a_1, a_2, \dots, a_v$  μικρότεροι του  $x$ .

Αν  $x = 10$  έχουμε το σε χρήση δεκαδικό σύστημα αρίθμησης και το  
σύμβολο  $[x]$  παραλείπεται.

Αν  $x = 2$  έχουμε το δυαδικό σύστημα αρίθμησης που χρησιμοποιείται  
στους ηλεκτρονικούς υπολογιστές.

Τον γεννήτορα τύπο του κριτηρίου διαιρετότητας του  $\frac{a}{[x]}$  διά  $\delta$  θα τον  
συμβολίζουμε με το σύμβολο  $T\left(\frac{a}{[x]}\right)$  και το κριτήριο διαιρετότητας με το  
σύμβολο  $T_\delta\left(\frac{a}{[x]}\right)$ .

Ο γεννήτορας τύπος  $T\left(\frac{a}{[x]}\right)$  είναι παράσταση η οποία περιέχει ψηφία  
του αριθμού, τμήματα αυτού και γράμματα (παραμέτρους) που συνδέονται  
με τα σύμβολα των πράξεων, όπως

$T\left(\frac{a}{[x]}\right) = a_v$ ,  $T\left(\frac{a}{[x]}\right) = \Sigma = \text{αθρ. ψηφίων του } \frac{a}{[x]}$ ,  $T\left(\frac{a}{[x]}\right) = \frac{\beta}{[x]} = \text{τμήμα των } \lambda$

τελευταίων ψηφίων του  $\frac{a}{[x]}$ ,  $T\left(\frac{a}{[x]}\right) = 5a_v + \overline{a_0 a_1 \dots a_{v-1}}$ ,

$$T\left(\frac{a}{[x]}\right) = u\alpha_v + \lambda \overline{\alpha_0 \alpha_1 \dots \alpha_{v-1}}, \quad T\left(\frac{a}{[x]}\right) = u \overline{\alpha_{v-1} \alpha_v} + \lambda \overline{\alpha_0 \alpha_1 \dots \alpha_{v-2}},$$

$$T\left(\frac{a}{[x]}\right) = u \overline{\alpha_{v-2} \alpha_{v-1} \alpha_v} + \lambda \overline{\alpha_0 \alpha_1 \dots \alpha_{v-3}}.$$

Οι τρεις τελευταίοι είναι παραμετρικοί με παραμέτρους  $u, \lambda$  (προσδιοριστέους) τα δε κριτήρια διαιρετότητας που παράγονται από αυτούς είναι αντίστοιχα

$$T_0\left(\frac{a}{[x]}\right) = u_0 \alpha_v + \lambda_0 \overline{\alpha_0 \alpha_1 \dots \alpha_{v-1}}, \quad T_0\left(\frac{a}{[x]}\right) = u_0 \overline{\alpha_{v-1} \alpha_v} + \lambda_0 \overline{\alpha_0 \alpha_1 \dots \alpha_{v-2}},$$

$$T_0\left(\frac{a}{[x]}\right) = u_0 \overline{\alpha_{v-2} \alpha_{v-1} \alpha_v} + \lambda_0 \overline{\alpha_0 \alpha_1 \dots \alpha_{v-3}} \quad \text{όπου } (u_0, \lambda_0) \text{ είναι μία λύση των}$$

Διοφαντικών εξισώσεων  $ux - \lambda = \text{πολδ}, ux^2 - \lambda = \text{πολδ}, ux^3 - \lambda = \text{πολδ}.$

Στα επόμενα, για λόγους συντομογραφίας θα γράφουμε: αντί κριτήριο διαιρετότητας, «Κ.Δ.», αντί σχέση ισοδυναμίας, «Σ.Ι.» και αντί Διοφαντική εξίσωση, «Δ.ε.»

**Σημείωση:** Η σχέση ισοτιμίας του  $\frac{a}{[x]}$  &  $T_0\left(\frac{a}{[x]}\right) \pmod{\delta}$  σημαίνει ότι οι

αριθμοί  $\frac{a}{[x]}$  και  $T_0\left(\frac{a}{[x]}\right)$  είναι ισοπόλοιποι όταν διαιρεθούν δια  $\delta$  ήτοι

$$\text{υπ:} \left(\frac{a}{[x]}, \delta\right) = \text{υπ:} \left(T_0\left(\frac{a}{[x]}\right), \delta\right).$$

**Α' Εύρεση των «Κ.Δ.», «Σ.Ι.», υπ:  $\left(\frac{a}{[x]}, \delta\right)$**

**Με τύπους μη παραμετρικούς (Α' μορφής)**

**1. Με τύπο  $T\left(\frac{a}{[x]}\right) = \alpha_v$**

**Θ1.** «Αν  $\delta \mid x$  τότε  $\delta \mid \frac{a}{[x]} \circ \delta \mid \alpha_v, \frac{a}{[x]} = T\left(\frac{a}{[x]}\right) \pmod{\delta}$  ή υπ:  $\left(\frac{a}{[x]}, \delta\right) =$

υπ:  $(T(\frac{a}{[x]}), \delta)$

$$\begin{aligned} \text{Αφού } \delta \mid x \downarrow x &= \text{πολ. } \delta, \frac{a}{[x]} = \alpha_0 x^v + \alpha_1 x^{v-1} + \dots + \alpha_{v-1} x + \alpha_v \\ &= (\alpha_0 x^{v-1} + \dots + \alpha_{v-1})x + \alpha_v = (\text{πολ}\delta) + \alpha_v = \text{πολ } \delta + T\left(\frac{a}{[x]}\right) \\ \text{Από την } \frac{a}{[x]} &= \text{πολ}\delta + T\left(\frac{a}{[x]}\right) \text{ προκύπτει } \delta \mid \frac{a}{[x]} \circ \delta \mid T\left(\frac{a}{[x]}\right), \frac{a}{[x]} - T\left(\frac{a}{[x]}\right) = \text{πολ}\delta \\ \frac{a}{[x]} &\& T\left(\frac{a}{[x]}\right) \pmod{\delta} \text{ ή υπ: } \left(\frac{a}{[x]}, \delta\right) = \text{υπ: } \left(T\left(\frac{a}{[x]}\right), \delta\right). \end{aligned}$$

**Σημείωση:** Επειδή ο γεννήτορας τύπος είναι μη παραμετρικός έπεται ότι  $T\left(\frac{a}{[x]}\right) = T_0\left(\frac{a}{[x]}\right) = \alpha_v$ .

*Όστε «Ένας αριθμός είναι διαιρετός με ένα διαιρέτη της βάσης του συστήματος αρίθμησης τότε και μόνο όταν διαιρεί το τελευταίο ψηφίο του αριθμού»*

π.χ. Αν  $\frac{a}{[x]} = \frac{3275}{[14]}$  και  $\delta = 7$ . Επειδή  $7 \mid 14$  έχουμε «Κ.Δ»  $T_0\left(\frac{3275}{[14]}\right) = 5$  και «Σ.Ι.»  $\frac{3275}{[14]} \& 5 \pmod{7}$  και υπ:  $\left(\frac{3275}{[14]}, 7\right) = \text{υπ: } (5, 7) = 5$ .

2. Αν  $T\left(\frac{a}{[x]}\right) = \frac{\beta}{[x]}$ , όπου  $\frac{\beta}{[x]}$  το τμήμα των  $\lambda$  τελευταίων ψηφίων του  $\frac{a}{[x]}$

**Θ2.** «Αν  $\delta \mid x$  τότε  $\delta^\lambda \mid \frac{a}{[x]} \circ \delta^\lambda \mid \frac{\beta}{[x]}$ ,  $\frac{a}{[x]} \& \frac{\beta}{[x]} \pmod{\delta^\lambda}$ ,

υπ:  $(\frac{a}{[x]}, \delta^\lambda) = \text{υπ: } (\frac{\beta}{[x]}, \delta^\lambda)$ ».

Αφού  $\delta \mid x \downarrow \delta^\lambda \mid x^\lambda$ . Αλλά  $\frac{a}{[x]} = \overline{\alpha_0 \alpha_1 \alpha_2 \dots \alpha_{v-\lambda}}_{[x]} x^\lambda + \overline{\alpha_{v-(\lambda-1)} \alpha_{v-(\lambda-2)} \dots \alpha_v}_{[x]}$  ή

$$\frac{a}{[x]} = \overline{\alpha_0 \alpha_1 \alpha_2 \dots \alpha_{v-\lambda}} \text{ πολ } (\delta^\lambda) + \frac{\beta}{[x]} \text{ ή } \frac{a}{[x]} = \text{πολ } (\delta^\lambda) + \frac{\beta}{[x]} \quad (1)$$

Από την (1) προκύπτει

$$\delta^\lambda \mid \binom{a}{[x]} \circ \delta^\lambda \mid \binom{\beta}{[x]}, \binom{a}{[x]} \& \binom{\beta}{[x]} \pmod{\delta^\lambda}, \text{ , υπ:} \left( \binom{a}{[x]}, \delta^\lambda \right) = \text{υπ:} \left( \binom{\beta}{[x]}, \delta^\lambda \right).$$

**Σημείωση:**  $T\left(\binom{a}{[x]}\right) = T_0\left(\binom{\beta}{[x]}\right) = \binom{\beta}{[x]}$

«Ένας αριθμός είναι διαιρετός με την  $\lambda$  δύναμη διαιρετή της βάσης τότε και μόνο όταν αυτή διαιρεί το τμήμα των  $\lambda$  τελευταίων ψηφίων του αριθμού».

π.χ. Αν  $\binom{a}{[x]} = \binom{56312}{[9]}$  και  $\delta = 3$ . Θα έχουμε για διαιρετή  $\Delta = 3^2$ .

«Κ.Δ.»  $T_0\left(\binom{56312}{[9]}\right) = \binom{312}{[9]} = 3,9^2 + 1,9 + 2 = 254,$

«Σ.Ι.»  $\binom{56312}{[9]} \& 254 \pmod{27}$  και υπ:  $\left(\binom{56312}{[9]}, 27\right) = \text{υπ:} (254, 27) = 11$

3. Αν  $T\left(\binom{a}{[x]}\right) = \Sigma$ , όπου  $\Sigma$  το άθροισμα των ψηφίων του  $\binom{a}{[x]}$ .

**Θ3.** «Αν  $\delta = x - 1$  τότε  $\delta \mid \binom{a}{[x]} \circ \delta \mid \Sigma$ ,  $\binom{a}{[x]} \& \Sigma \pmod{\delta}$ ,

υπ:  $\left(\binom{a}{[x]}, \delta\right) = \text{υπ:} (\Sigma, \delta)$ »

Αφού  $\delta = x - 1 \downarrow x = \delta + 1 \downarrow x^\mu = (\delta + 1)^\mu = \text{πολ } \delta + 1 \text{ ! } \mu \in \mathbb{N}$

$$\binom{a}{[x]} = \alpha_0 x^\nu + \alpha_1 x^{\nu-1} + \dots + \alpha_{\nu-1} x + \alpha_\nu$$

$$= \alpha_0 (\text{πολ } \delta + 1) + \alpha_1 (\text{πολ } \delta + 1) + \dots + \alpha_{\nu-1} (\text{πολ } \delta + 1) + \alpha_\nu$$

$$= \text{πολ } \delta + (\alpha_0 + \alpha_1 + \alpha_2 + \dots + \alpha_{\nu-1} + \alpha_\nu) \text{ ή } \binom{a}{[x]} = \text{πολ } \delta + \Sigma \quad (1)$$

Από την (1) προκύπτει:

«Κ.Δ.»  $\delta \mid \binom{a}{[x]} \circ \delta \mid \Sigma$ , «Σ.Ι.»  $\binom{a}{[x]} \& \Sigma \pmod{\delta}$ , υπ:  $\left(\binom{a}{[x]}, \delta\right) = \text{υπ:} (\Sigma, \delta)$

«Ένας αριθμός είναι διαιρετός με τον  $(x-1)$  τότε και μόνο όταν αυτός διαιρεί το άθροισμα των ψηφίων του αριθμού».

π.χ. Αν  $\binom{a}{[x]} = \overline{2\alpha_0 3\alpha_2}_{[15]}$  και  $\delta = 14$ . Επειδή  $\delta = 14 \mid x - 1$  ισχύουν

$$\text{«ΚΔ» } 14 \mid \overline{2\alpha_0 3\alpha_2}_{[15]} \circ 14 \mid 2 + \alpha_0 + 3 + \alpha_2 = 2 + 10 + 3 + 12 = 27,$$

$$\text{«Σ.Β» } \overline{2\alpha_0 3\alpha_2}_{[15]} \& 27 \pmod{14} \text{ και}$$

$$\text{υπ: } \left( \overline{2\alpha_0 3\alpha_2}_{[15]}, 14 \right) = \text{υπ: } (\Sigma, 14) = \text{υπ: } (27, 14) = 13.$$

$$\text{Σημείωση: } \text{Επειδή } 14 \uparrow \Sigma = 27 \downarrow 14 \uparrow \overline{2\alpha_0 3\alpha_2}_{[15]}.$$

$$\left( \overline{2\alpha_0 3\alpha_2}_{[15]} = 9057 = 14 \cdot 646 + 13 \right)$$

4. Αν  $T\left(\frac{a}{[x]}\right) = \Sigma$ , όπου  $\Sigma$  το άθροισμα των 2ψήφιων τμημάτων του  $\frac{a}{[x]}$  (από δεξιά)

Θ4. «Αν  $\delta = x + 1$  τότε  $\delta \mid \frac{a}{[x]} \circ \delta \mid \Sigma, \frac{a}{[x]} \& \Sigma \pmod{\delta}$ ,

$$\text{υπ: } \left( \frac{a}{[x]}, \delta \right) = \text{υπ: } (\Sigma, \delta)»$$

$$\text{Αφού } \delta = x + 1 \circ x = \delta - 1 \downarrow x^2 = (\delta - 1)^2 \downarrow x^2 = \text{πολ}\delta + 1$$

Ο  $\frac{a}{[x]} = \overline{\alpha_0 \alpha_1 \alpha_2 \dots \alpha_n}_{[x]}$  χωριζόμενος σε 2ψήφια τμήματα γράφεται

Αν  $n = \text{περιττός}$ :

$$\begin{aligned} \frac{a}{[x]} = & \overline{\alpha_0 \alpha_1}_{[x]} (x^2)^{\frac{n-1}{2} - 1} + \overline{\alpha_2 \alpha_3}_{[x]} (x^2)^{\frac{n-1}{2} - 2} + \overline{\alpha_4 \alpha_5}_{[x]} (x^2)^{\frac{n-1}{2} - 3} \\ & + \dots + \overline{\alpha_{n-3} \alpha_{n-2}}_{[x]} (x^2)^1 + \overline{\alpha_{n-1} \alpha_n}_{[x]} \end{aligned}$$

$$\begin{aligned}
&= \overline{\alpha_0 \alpha_1}_{[x]} (\text{πολ}\delta + 1) + \overline{\alpha_2 \alpha_3}_{[x]} (\text{πολ}\delta + 1) + \overline{\alpha_4 \alpha_5}_{[x]} (\text{πολ}\delta + 1) \\
&\quad + \dots + \overline{\alpha_{v-3} \alpha_{v-2}}_{[x]} (\text{πολ}\delta + 1) + \overline{\alpha_{v-1} \alpha_v}_{[x]} \\
&= \text{πολ}\delta + \Sigma \quad (1)
\end{aligned}$$

Αν  $v = \acute{\alpha}$ ρτιος:

$$\begin{aligned}
\overline{a}_{[x]} &= \alpha_0 (x^2)^{\frac{v}{2}} + \overline{\alpha_1 \alpha_2}_{[x]} (x^2)^{\frac{v}{2}-1} + \overline{\alpha_3 \alpha_4}_{[x]} (x^2)^{\frac{v}{2}-2} + \dots + \overline{\alpha_{v-3} \alpha_{v-2}}_{[x]} (x^2)^1 + \overline{\alpha_{v-1} \alpha_v}_{[x]} \\
&= \text{πολ}\delta + \Sigma \quad (2)
\end{aligned}$$

Από τις (1) και (2) προκύπτει :

«Κ.Δ.»  $\delta \mid \overline{a}_{[x]} \circ \delta \mid \Sigma$ , «Σ.Ι.»  $\overline{a}_{[x]} \& \Sigma \pmod{\delta}$ , υπ:  $\left( \overline{a}_{[x]}, \delta \right) = \text{υπ: } (\Sigma, \delta)$ .

*«Ένας αριθμός είναι διαιρετός με τον  $(x + 1)$  τότε και μόνο όταν αυτός διαιρεί το άθροισμα των 2ψηφίων τμημάτων του αριθμού».*

π.χ. Αν  $\overline{a}_{[x]} = \overline{208\alpha_3 5}_{[14]}$  και  $\delta = 15$ . Επειδή  $\delta \mid x + 1$  και

$$\Sigma = 2 + \overline{08}_{[14]} + \overline{\alpha_3 5}_{[x]} = 197 \text{ έχουμε το } T_0 \left( \overline{208\alpha_3 5}_{[14]} \right) = \Sigma = 197,$$

$$\text{«Σ.Ι.» } \overline{208\alpha_3 5}_{[14]} = \Sigma \pmod{15}, \text{ υπ: } \left( \overline{208\alpha_3 5}_{[14]}, 15 \right) = \text{υπ: } (\Sigma, 15) = 2.$$

**Συμπέρασμα:** Ισχύουν για τους τύπους Α. μορφής  $T \left( \overline{a}_{[x]} \right) = T_0 \left( \overline{a}_{[x]} \right)$

και  $\overline{a}_{[x]} \& T \left( \overline{a}_{[x]} \right) \pmod{\delta}$ .

Υπάρχουν πάρα πολλά κριτήρια διαιρετότητας ενός αριθμού  $\overline{a}_{[x]}$  με κάθε διαιρέτη  $\delta$ , αλλά δεν είναι εύκολο να τα μαντεύσουμε.

Για να βρούμε το «Κ.Δ.»  $T \left( \overline{a}_{[x]} \right)$ , τη «Σ.Ι.»  $\overline{a}_{[x]} \& T_0 \left( \overline{a}_{[x]} \right) \pmod{\delta}$

και το υπ:  $\left(\frac{a}{[x]}, \delta\right)$ , επινόησα τους παραμετρικούς γεννήτορες τύπους κριτηρίων διαιρετότητας με τις αντίστοιχες αυτών Διοφαντικές εξισώσεις που αναφέρονται στην εισαγωγή.

**B. Εύρεση των «Κ.Δ.», «Σ.Ι.», υπ:  $\left(\frac{a}{[x]}, \delta\right)$**

**Με γεννήτορες τύπους παραμετρικούς (B. μορφής)**

1. Με τύπο  $T\left(\frac{a}{[x]}\right) = u\alpha_v + \lambda \frac{\overline{\alpha_0 \alpha_1 \dots \alpha_{v-1}}}{[x]}$

$$\frac{a}{[x]} = \frac{\overline{\alpha_0 \alpha_1 \dots \alpha_v}}{[x]} = \frac{\overline{\alpha_0 \alpha_1 \dots \alpha_{v-1}}}{[x]} x + \alpha_v \downarrow u \frac{a}{[x]} = ux \frac{\overline{\alpha_0 \alpha_1 \dots \alpha_{v-1}}}{[x]} + u\alpha_v$$

$$\downarrow u \frac{a}{[x]} = (ux - \lambda) \frac{\overline{\alpha_0 \alpha_1 \dots \alpha_{v-1}}}{[x]} + u\alpha_v + \lambda \frac{\overline{\alpha_0 \alpha_1 \dots \alpha_{v-1}}}{[x]}$$

$$\downarrow u \frac{a}{[x]} = (ux - \lambda) \frac{\overline{\alpha_0 \alpha_1 \dots \alpha_{v-1}}}{[x]} + T\left(\frac{a}{[x]}\right) \quad (1)$$

Η (1) μας υποδεικνύει να θέσουμε  $ux - \lambda = \text{πολ } \delta$  με  $(u, \delta) = 1$  (2)  
 Αν  $(u_0, \lambda_0)$  είναι μία λύση της «Δ.ε» (2), ο γεννήτορας τύπος δίδει

$$T_0\left(\frac{a}{[x]}\right) = u_0 \alpha_v + \lambda_0 \frac{\overline{\alpha_0 \alpha_1 \dots \alpha_{v-1}}}{[x]}$$

Αν  $(u_0, \lambda_0) = (1, \lambda_0) = (1, x - \text{πολ}\delta) = (1, x - \kappa\delta)$ , ο γεννήτορας τύπος δίδει  $T_0\left(\frac{a}{[x]}\right) = \alpha_v + (x - \kappa\delta) \frac{\overline{\alpha_0 \alpha_1 \dots \alpha_{v-1}}}{[x]}$ .

Η (1) γίνεται αντίστοιχα  $u_0 \frac{a}{[x]} = \text{πολ } \delta + T_0\left(\frac{a}{[x]}\right)$  (α) και

$$\frac{a}{[x]} = \alpha_v + T_0\left(\frac{a}{[x]}\right) \quad (\beta) \quad (3)$$

Επειδή  $(u, \delta) = 1$  και  $(1, \delta) = 1$ , από τις (3) λαμβάνουμε αντίστοιχα

$$\alpha) \quad \text{«ΚΔ» } \left[ \delta \mid \frac{a}{[x]} \circ \delta \mid T_0\left(\frac{a}{[x]}\right) \right], \text{ «ΣΙ» } \left[ u \frac{a}{[x]} \& T_0\left(\frac{a}{[x]}\right) \pmod{\delta} \right]$$

όταν  $(u = u_0, \delta) = 1$  και  $u_0 \neq 1$

$$\beta) \text{ «ΚΔ» } \boxed{\delta \mid \frac{a}{[x]} \circ \delta \mid T_0\left(\frac{a}{[x]}\right)}, \text{ «ΣΙ» } \boxed{\frac{a}{[x]} \& T_0\left(\frac{a}{[x]}\right) \pmod{\delta}}$$

όταν  $\boxed{u_0 = 1}$  και υπ:  $\left(\frac{a}{[x]}, \delta\right) = \text{υπ: } \left(T_0\left(\frac{a}{[x]}\right), \delta\right)$ .

π.χ. Να βρεθεί ένα «Κ.Δ.» του  $a$  δια 13, όταν  $a = \overline{a_0 a_1 \dots a_n}$ .

Επειδή  $x = 10$ ,  $\delta = 13$  η αντίστοιχη του τύπου «Δ.ε» είναι  $u, 10 - \lambda = \text{πολ } 13 \text{ με } (u, \delta) = 1$

Μία λύση αυτής είναι  $(u_0, \lambda_0) = (4, 1)$ . Επομένως

$$\boxed{T_0(a) = 4a_n + 1, \overline{a_0 a_1 \dots a_{n-1}}}$$

Δια  $a = 25317$  έχουμε  $T_0(25317) = 4,7 + 2531 = 2559 = \tau_1$  1<sup>ο</sup> βήμα  
Επειδή ο αριθμός  $\tau_1 = 2559$  είναι μεγάλος, εφαρμόζουμε το «Κ.Δ.» δια  $2^3 \cdot 3^3$  κ.λπ. φορά έως ότου βρούμε αριθμό μικρό ώστε να διαπιστώσουμε αν αυτός διαιρείται.

$$\begin{aligned} T_0(\tau_1) &= T_0(2559) = 4,9 + 255 = 291 = \tau_2 && 2^\circ \text{ βήμα} \\ T_0(\tau_2) &= T_0(291) = 4,1 + 29 = 33 = \tau_3 && 3^\circ \text{ βήμα} \end{aligned}$$

Επειδή  $13 \nmid 33 \downarrow 13 \nmid 25317$

**Σημείωση:** Όταν ο αριθμός  $a$  δεν είναι διαιρετός δια  $\delta$  (όπως στο παράδειγμα) η «Σ.Ι.» ισχύει μόνο για το 1<sup>ο</sup> βήμα: Έτσι  $4,25317 \& 2559 \pmod{13}$

$$2. \text{ Με τύπο } T\left(\frac{a}{[x]}\right) = u \frac{\overline{a_{n-1} a_n}}{[x]} + \lambda \frac{\overline{a_0 a_1 \dots a_{n-2}}}{[x]}$$

$$\frac{a}{[x]} = \frac{\overline{a_0 a_1 \dots a_n}}{[x]} = \frac{\overline{a_0 a_1 \dots a_{n-2}}}{[x]} \cdot x^2 + \frac{\overline{a_{n-1} a_n}}{[x]} \downarrow u \frac{a}{[x]} = ux^2 \frac{\overline{a_0 a_1 \dots a_{n-2}}}{[x]} + u \frac{\overline{a_{n-1} a_n}}{[x]} \downarrow$$

$$u \frac{a}{[x]} = (ux^2 - \lambda) \frac{\overline{a_0 a_1 \dots a_{n-2}}}{[x]} + u \frac{\overline{a_{n-1} a_n}}{[x]} + \lambda \frac{\overline{a_0 a_1 \dots a_{n-2}}}{[x]} \downarrow$$

$$u \frac{a}{[x]} = (ux^2 - \lambda) \overline{a_0 a_1 \dots a_{v-2}} + T_0 \left( \frac{a}{[x]} \right) \quad (1)$$

Η (1) υποδεικνύει να θέσουμε  $ux^2 - \lambda = \text{πολ } \delta$  με  $(u, \delta) = 1$  (2)  
 Αν  $(u_0, \lambda_0)$  είναι μία λύση της «Δ.ε» (2), ο γεννήτορας τύπος δίδει:

$$T_0 \left( \frac{a}{[x]} \right) = u_0 \overline{a_{v-1} a_v} + \lambda_0 \overline{a_0 a_1 \dots a_{v-2}}$$

Αν  $(u_0, \lambda_0) = (1, \lambda_0) = (1, x^2 - \text{πολ } \delta)$ , ο γεννήτορας τύπος δίδει:

$$T_0 \left( \frac{a}{[x]} \right) = \overline{a_{v-1} a_v} + (x^2 - \text{πολ } \delta) \overline{a_0 a_1 \dots a_{v-2}}$$

Η (1) γίνεται αντίστοιχα:  $u_0 \frac{a}{[x]} = \text{πολ } \delta + T_0 \left( \frac{a}{[x]} \right)$  (α)

και  $\frac{a}{[x]} = \text{πολ } \delta + T_0 \left( \frac{a}{[x]} \right)$  (β) (3)

Επειδή  $(u, \delta) = 1$  και  $(1, \delta) = 1$ , από τις (α) και (β) της (3) λαμβάνουμε αντίστοιχα:

α) «Κ.Δ»  $\delta \mid \frac{a}{[x]} \circ \delta \mid T_0 \left( \frac{a}{[x]} \right)$ , «ΣΙ»  $u \frac{a}{[x]} \& T_0 \left( \frac{a}{[x]} \right) \pmod{\delta}$

όταν  $(u = u_0, \delta) = 1$  και  $u_0 \neq 1$

β) «Κ.Δ»  $\delta \mid \frac{a}{[x]} \circ \delta \mid T_0 \left( \frac{a}{[x]} \right)$ , «ΣΙ»  $\frac{a}{[x]} \& T_0 \left( \frac{a}{[x]} \right) \pmod{\delta}$

όταν  $u = u_0 = 1$  και υπ:  $\left( \frac{a}{[x]}, \delta \right) = \text{υπ:} \left( T_0 \left( \frac{a}{[x]} \right), \delta \right)$ .

**Παράδειγμα 1.**

Να βρεθεί ένα «Κ.Δ» του  $a$  δια 7, η «Σ.Ι» και υπ:  $(a, 7)$  όταν  $a = 8325$ .

Η αντίστοιχη του τύπου «Δ.ε» είναι:  $u \cdot 10^2 - \lambda = \text{πολ } 7$  με  $(u, 7) = 1$ .

Αυτή έχει λύση την  $(u_0, \lambda_0) = (1, 2)$ . Επειδή  $u_0 = 1$  θα έχουμε

$$T_0(a) = \overline{a_{v-1} a_v} + 2 \overline{a_0 a_1 \dots a_{v-2}}, \quad a = T_0(a) \pmod{7}, \quad \text{υπ:} (a, 7) = \text{υπ:} (T_0(a), 7)$$

και  $T_0(8325) = 25 + 2 \cdot 83 = 191, \quad 8325 \& 191 \pmod{7},$

υπ:  $(8325, 7) = \text{υπ:} (191, 7) = 2$

*Ώστε: «Ένας αριθμός του 10-δικού συστήματος αρίθμησης, είναι διαιρετός με τον 7 τότε και μόνο όταν ο 7 διαιρεί το άθροισμα του τελευταίου 2ψηφίου τμήματος του αριθμού και του 2πλασίου γινομένου των εκατοντάδων του αριθμού».*

### Παράδειγμα 2

Να βρεθεί ένα «Κ.Δ» του  $\frac{a}{[5]} = \frac{240132}{[5]}$  δια του 7, η «Σ.Ι» και το

$$\text{υπ:} \left( \frac{a}{[5]}, 7 \right).$$

Η αντίστοιχη του γεννήτορα τύπου «Δ.ε» είναι  $u, 5^2 - \lambda = \text{πολ}7$  με  $(u, 7) = 1$  η οποία έχει τη λύση  $(u_0, \lambda_0) = (1, 4)$ .

$$\text{Έτσι έχουμε } T_0 \left( \frac{240132}{[5]} \right) = \frac{32}{[5]} + 4, \frac{2401}{[5]} = \frac{32}{[5]} + \frac{21104}{[5]} = \frac{21141}{[5]}$$

Επειδή  $u_0 = 1$ , «Σ.Ι» (mod7) είναι  $\frac{240132}{[5]} \& \frac{21141}{[5]}$  και

$$\text{υπ:} \left( \frac{a}{[5]}, 7 \right) = \text{υπ:} \left( \frac{21141}{[5]}, 7 \right) = 0.$$

$$3. \text{ Με τύπο } T \left( \frac{a}{[x]} \right) = u \frac{\overline{a_{v-2} a_{v-1} a_v}}{[x]} + \lambda \frac{\overline{a_0 a_1 \dots a_{v-3}}}{[x]}$$

$$\frac{a}{[x]} = \frac{\overline{a_0 a_1 \dots a_v}}{[x]} = \frac{\overline{a_0 a_1 \dots a_{v-3}}}{[x]} x^3 + \frac{\overline{a_{v-2} a_{v-1} a_v}}{[x]} \downarrow u \frac{a}{[x]} = ux^3, \frac{\overline{a_0 a_1 \dots a_{v-3}}}{[x]} +$$

$$u \frac{\overline{a_{v-2} a_{v-1} a_v}}{[x]} \downarrow$$

$$u \frac{a}{[x]} = (ux^3 - \lambda) \frac{\overline{a_0 a_1 \dots a_{v-3}}}{[x]} + u \left( \frac{\overline{a_{v-2} a_{v-1} a_v}}{[x]} + \lambda \frac{\overline{a_0 a_1 \dots a_{v-3}}}{[x]} \right) \downarrow$$

$$u \frac{a}{[x]} = (ux^3 - \lambda) \frac{\overline{a_0 a_1 \dots a_{v-3}}}{[x]} + T \left( \frac{a}{[x]} \right) \quad (1)$$

$$\text{Θέτουμε } ux^3 - \lambda = \text{πολ } \delta \text{ με } (u, \delta) = 1 \quad (2)$$

Αν  $(u_0, \lambda_0)$  είναι μία λύση της «Δ.ε» (2), τότε

$$T_0\left(\frac{a}{[x]}\right) = u_0 \overline{a_{v-2} a_{v-1} a_v}_{[x]} + \lambda_0 \overline{a_0 a_1 \dots a_{v-3}}_{[x]}$$

Αν  $(u_0, \lambda_0) = (1, \lambda_0) = 1, x^3 - \text{πολ}\delta$  τότε

$$T_0\left(\frac{a}{[x]}\right) = \overline{a_{v-2} a_{v-1} a_v}_{[x]} + (x^3 - \text{πολ}\delta) \overline{a_0 a_1 \dots a_{v-3}}_{[x]}$$

Η (1) γίνεται  $u_0 \frac{a}{[x]} = \text{πολ}\delta + T_0\left(\frac{a}{[x]}\right)$  αν  $u_0 \neq 1$

και  $\frac{a}{[x]} = \text{πολ}\delta + T_0\left(\frac{a}{[x]}\right)$  αν  $u_0 = 1$  (3)

Επειδή  $(u_0, \delta) = 1$  από τις (3) λαμβάνουμε:

α) Αν  $u_0 \neq 1$ : «Κ.Δ»  $\delta \mid \frac{a}{[x]} \circ \delta \mid T_0\left(\frac{a}{[x]}\right)$ , «Σ.Ι»  $u_{[x]} \frac{a}{[x]} \& T_0\left(\frac{a}{[x]}\right) \pmod{\delta}$

β) Αν  $u_0 = 1$ : «Κ.Δ»  $\delta \mid \frac{a}{[x]} \circ \delta \mid T_0\left(\frac{a}{[x]}\right)$ , «Σ.Ι»  $u_{[x]} \frac{a}{[x]} \& T_0\left(\frac{a}{[x]}\right) \pmod{\delta}$

και υπ:  $\left(\frac{a}{[x]}, \delta\right) = \text{υπ:} \left(T_0\left(\frac{a}{[x]}\right), \delta\right)$

**Παράδειγμα**

Να βρεθεί το «Κ.Δ» δια 17 στο 10-δικό σύστημα και το υπ: (90451, 17).

Η αντίστοιχη του τύπου «Δ.ε» είναι  $u, x^3 - \lambda = \text{πολ}\delta$  με  $(u, \delta) = 1$ .

Για  $x = 10, \delta = 17$  γίνεται  $u, 10^3 - \lambda = \text{πολ} 17$ .

Επειδή ζητείται το υπ:  $(a, \delta)$ , θα βρούμε τη λύση  $(u_0, \lambda_0) = (1, \lambda_0)$ . Αυτή είναι  $(1, 14)$ .

$T_0(a) = \overline{1, a_{v-2} a_{v-1} a_v} + 14, \overline{a_0 a_1 \dots a_{v-3}}$  ή  $T_0(a) = \overline{a_{v-2} a_{v-1} a_v} + 14, \overline{a_0 a_1 \dots a_{v-3}}$

Επειδή «Σ.Ι» είναι  $a \& T_0(a) \pmod{\delta}$  όταν  $u_0 = 1$  θα έχουμε υπ:  $(a, \delta) = \text{υπ:} (T_0(a), \delta)$ .

Για  $a = 90451, \delta = 17$  και  $(u_0, \lambda_0) = (1, 14)$  έχουμε

$T_0(a) = 451 + 14,90 = 451 + 1260 = 1711$ . Επειδή  $17 \nmid 1711 \downarrow 17 \nmid 90451$  έχουμε υπ:  $(90451, 17) = \text{υπ:} (1711, 17) = 11$ .

**Συμπεράσματα**

- 1<sup>ο</sup> Η εύρεση των «Κ.Δ» ανάγεται στην επίλυση των Διοφαντικών εξισώσεων α' βαθμού  $ux - \lambda = \text{πολ}\delta$ ,  $ux^2 - \lambda = \text{πολ}\delta$ ,  $ux^3 - \lambda = \text{πολ}\delta$  (με αγνώστους  $u, \lambda$ )
- 2<sup>ο</sup> Επειδή οι εξισώσεις έχουν άπειρες λύσεις και τα «Κ.Δ» του  $\frac{a}{[x]}$  δια  $\delta$  είναι άπειρα.  
Από αυτά επιλέγουμε το απλούστερο κατά περίπτωση.
- 3<sup>ο</sup> Οι γεννήτορες παραμετρικοί τύποι, μετά τον προσδιορισμό των παραμέτρων, δίδουν «Κ.Δ» της Α' μορφής (χωρίς παράμετρο).
- 4<sup>ο</sup> Η ισοτιμία  $\frac{a}{[x]} \& T_0(\frac{a}{[x]})$  αντιστοιχεί στη λύση  $(u_0, \lambda_0) = (1, \lambda_0)$ , της αντίστοιχης του τύπου «Δ.ε»
- 5<sup>ο</sup> Ο γενικός τύπος του «Κ.Δ» φανερώνει αφ' ενός μεν τη μορφή του  $T(\frac{a}{[x]})$ , αφ' ετέρου δε τη λύση  $(u_0, \lambda_0)$  της αντίστοιχης «Δ.ε» που πήραμε για την εύρεσή του.

Γεννήτορες Τύποι	Διοφαντικές Εξισώσεις	Γενικοί τύποι «Κ.Δ»	«Σ.Ι» (mod $\delta$ )	
			$u_0 \neq 0$	$u_0 = 1, \delta \mid \frac{a}{[x]}$
$T(\frac{a}{[x]}) = ua_0 + \lambda \frac{\overline{a_0 a_1 \dots a_{n-1}}}{[x]}$	$ux - \lambda = \text{πολ}\delta$	$T_0(\frac{a}{[x]}) = u_0 a_0 + \lambda \frac{\overline{a_0 a_1 \dots a_{n-1}}}{[x]}$	$u \frac{a}{[x]} \& T_0(\frac{a}{[x]})$	$\frac{a}{[x]} \& T_0(\frac{a}{[x]})$
$T(\frac{a}{[x]}) = u \frac{\overline{a_{n-1} a_n}}{[x]} + \lambda \frac{\overline{a_0 a_1 \dots a_{n-1}}}{[x]}$	$ux^2 - \lambda = \text{πολ}\delta$	$T_0(\frac{a}{[x]}) = u_0 \frac{\overline{a_{n-1} a_n}}{[x]} + \lambda_0 \frac{\overline{a_0 a_1 \dots a_{n-1}}}{[x]}$	»	»
$T(\frac{a}{[x]}) = u \frac{\overline{a_{n-2} a_{n-1} a_n}}{[x]} + \lambda \frac{\overline{a_0 a_1 \dots a_{n-1}}}{[x]}$	$ux^3 - \lambda = \text{πολ}\delta$	$T_0(\frac{a}{[x]}) = u_0 \frac{\overline{a_{n-2} a_{n-1} a_n}}{[x]} + \lambda_0 \frac{\overline{a_0 a_1 \dots a_{n-1}}}{[x]}$	»	»

$+ \lambda \overline{a_0 a_1 \dots a_{n-1}}_{[x]}$		$\lambda_0 \overline{a_0 a_1 \dots a_{n-1}}_{[x]}$		
Αν $u_0 = 1$ ή $\delta \mid \overline{a}_{[x]}$ τότε ισχύει: $\left( \overline{a}_{[x]} \delta \right) = \text{ισχ:} \left( T_0 \left( \overline{a}_{[x]} \right), \delta \right)$				

### Ειδικές σχέσεις ισοτιμίας (mod $\delta$ )

Αν  $\overline{a}_{[x]} = \overline{a_0 a_1 \dots a_{n-1}}_{[x]}$  και  $\overline{\beta}_{[x]} = \overline{\beta_0 \beta_1 \dots \beta_{n-1}}_{[x]}$  με «Κ.Δ»  $T_0(\overline{a}_{[x]}), T_0'(\overline{\beta}_{[x]})$  τότε:

- Αν  $\delta \mid \overline{a}_{[x]}$  και  $\delta \mid \overline{\beta}_{[x]}$   $\downarrow \overline{a}_{[x]} + \overline{\beta}_{[x]} \ \& \ T_0(\overline{a}_{[x]}) + T_0'(\overline{\beta}_{[x]})$   
και  $\overline{a}_{[x]} \overline{\beta}_{[x]} \ \& \ T_0(\overline{a}_{[x]}), T_0'(\overline{\beta}_{[x]}) \pmod{\delta}$
- Αν  $\delta \mid \overline{a}_{[x]}$  και  $\delta \nmid \overline{\beta}_{[x]}$   $\downarrow \overline{a}_{[x]} + u_0' \overline{\beta}_{[x]} \ \& \ T_0(\overline{a}_{[x]}) + T_0'(\overline{\beta}_{[x]})$   
και  $u_0' \overline{a}_{[x]} \overline{\beta}_{[x]} \ \& \ T_0(\overline{a}_{[x]}), T_0'(\overline{\beta}_{[x]}) \pmod{\delta}$
- Αν  $\delta \nmid \overline{a}_{[x]}$  και  $\delta \nmid \overline{\beta}_{[x]}$   $\downarrow u_0 \overline{a}_{[x]} + u_0' \overline{\beta}_{[x]} \ \& \ T_0(\overline{a}_{[x]}) + T_0'(\overline{\beta}_{[x]})$   
και  $u_0 u_0' \overline{a}_{[x]} \overline{\beta}_{[x]} \ \& \ T_0(\overline{a}_{[x]}), T_0'(\overline{\beta}_{[x]}) \pmod{\delta}$

### Απόδειξη της 2

Επειδή  $\delta \mid \overline{a}_{[x]}$  και  $\delta \nmid \overline{\beta}_{[x]}$   $\downarrow \overline{a}_{[x]} \ \& \ T_0(\overline{a}_{[x]})$  και  $u_0' \overline{\beta}_{[x]} \ \& \ T_0'(\overline{\beta}_{[x]}) \pmod{\delta}$

Με πρόσθεση και πολλαπλασιασμό κατά μέλη λαμβάνουμε:

$$\overline{a}_{[x]} + u_0' \overline{\beta}_{[x]} \ \& \ T_0(\overline{a}_{[x]}) + T_0'(\overline{\beta}_{[x]}) \text{ και } u_0' \overline{a}_{[x]} \overline{\beta}_{[x]} \ \& \ T_0(\overline{a}_{[x]}), T_0'(\overline{\beta}_{[x]}) \pmod{\delta}$$

- Αν  $\delta \nmid \overline{a}_{[x]}$  τότε  $u_0' \overline{a}_{[x]} \ \& \ \tau_{\delta}(\overline{a}_{[x]}) \pmod{\delta}$ , όταν η διαπίστωση της διαιρετότητας του  $\overline{a}_{[x]} : \delta$ , γίνεται κατά  $\mu^{\circ}$  εφαρμογή του «Κ.Δ»

Έστωσαν οι  $\mu$  διαδοχικές εφαρμογές του «Κ.Δ»

$$T_0\left(\frac{a}{[x]}\right) = \frac{\tau_1}{[x]}, T_0\left(\frac{\tau_1}{[x]}\right) = \frac{\tau_2}{[x]}, \dots, T_0\left(\frac{\tau_{\mu-1}}{[x]}\right) = \frac{\tau_\mu}{[x]}, T_0\left(\frac{\tau_\mu}{[x]}\right)$$

Επειδή  $\delta \uparrow \frac{a}{[x]} \downarrow u_0 \frac{a}{[x]} \& \frac{\tau_1}{[x]} \pmod{\delta}$  και  $\delta \uparrow \frac{\tau_1}{[x]}$  (1) φορά

Επειδή  $\delta \uparrow \frac{\tau_1}{[x]} \downarrow u_0 \frac{\tau_1}{[x]} \& \frac{\tau_2}{[x]} \pmod{\delta}$  και  $\delta \uparrow \frac{\tau_2}{[x]}$  (2) φορά

Επειδή  $\delta \uparrow \frac{\tau_2}{[x]} \downarrow u_0 \frac{\tau_2}{[x]} \& \frac{\tau_3}{[x]} \pmod{\delta}$  και  $\delta \uparrow \frac{\tau_3}{[x]}$  (3) φορά

...

Επειδή  $\delta \uparrow \frac{\tau_{\mu-1}}{[x]} \downarrow u_0 \frac{\tau_{\mu-1}}{[x]} \& \frac{\tau_\mu}{[x]} \pmod{\delta}$  και  $\delta \uparrow \frac{\tau_\mu}{[x]}$  ( $\mu$ ) φορά

---


$$u_0^\mu \frac{a}{[x]}, \frac{\tau_1}{[x]}, \frac{\tau_2}{[x]}, \frac{\tau_3}{[x]}, \dots, \frac{\tau_{\mu-1}}{[x]} \& \frac{\tau_1}{[x]}, \frac{\tau_2}{[x]}, \frac{\tau_3}{[x]}, \dots, \frac{\tau_\mu}{[x]} \downarrow \boxed{u_0^\mu \frac{a}{[x]} \& \frac{\tau_\mu}{[x]} \pmod{\delta}}$$

### Σημείωση

Αν  $\delta \mid \frac{a}{[x]}$  τότε  $\frac{a}{[x]} \& \frac{\tau_\mu}{[x]} \pmod{\delta} \neq \mu$ .