Θεμέλια των Μαθηματικών

Ελένη Τζανάκη & Θεόδουλος Γαρεφαλάκης

Εαρινο εξάμηνο 2019-20

Ορισμός κοινού διαιρέτη

Ένας ακέραιος d ονομάζεται κοινός διαιρέτης των $a, b \in \mathbb{Z}$ εάν $d \mid a$ και $d \mid b$.

Ορισμός μέγιστου κοινού διαιρέτη

Ένας ακέραιος d ονομάζεται (ένας) μέγιστος κοινός διαιρέτης (μκδ) των $a, b \in \mathbb{Z}$ εάν:

1. $d \mid a, \quad d \mid b$
2. Για κάθε $d' \in \mathbb{Z}$, αν $d' \mid a$ και $d' \mid b$ τότε $d' \mid d$.

Παρατηρήσεις:

- Δεν είναι προφανές ότι υπάρχει πάντα μκδ δύο ακεραίων a, b.
- Υπάρχει μοναδικός μκδ των 0, 0 και είναι το 0.

- Αν ο d είναι κοινός διαιρέτης των a, b, το ίδιο ισχύει για τον $-d$.

- Αν ο d είναι μέγιστος κοινός διαιρέτης των a, b, το ίδιο ισχύει για τον $-d$.
  - $-d \mid a$ και $-d \mid b$ (διότι $d \mid a$ και $d \mid b$).
  - Έστω ότι $d' \mid a$ και $d' \mid b$.
  - Τότε $d' \mid d$ (διότι ο d είναι μέγιστος κοινός διαιρέτης).
  - Άρα $d' \mid -d$.
- Εάν d και d' είναι δύο μκδ των a, b, τότε $d' \in \{d, -d\}$
  - $d' \mid a,\ d' \mid b$ (αφού ο d' είναι μκδ θα είναι και κοινός διαιρέτης),
  - άρα $d' \mid d$ (αφού ο d είναι μκδ διαιρείται από κάθε κοινό διαιρέτη).
  - Όμοια, $d \mid d'$.
  - Άρα $d' = d$ ή $d' = -d$.
- Μέγιστος κοινός διαιρέτης, όταν υπάρχει, *δεν* είναι μοναδικός.
- Για να τον "κάνουμε" μοναδικό κάνουμε την εξής σύμβαση: όταν λέμε "ο μέγιστος κοινός διαιρέτης των a, b" (εφόσον υπάρχει) εννοούμε το θετικό από τους δύο ακεραίους.
- Συμβολίζουμε το μκδ των a, b (εφόσον υπάρχει) με (a, b).

Πρόταση

Έστω $a, b \in \mathbb{Z}$. Τοτε $(a, b) = (b, a - qb)$, για οποιοδήποτε ακέραιο q.

Ας υποθέσουμε ότι $d = (a, b)$. Θα δείξουμε ότι $d = (a - qb, b)$.

- $d \mid a$ και $d \mid b$ οπότε $d \mid a - qb$.
- Έστω $d' \mid b$ και $d' \mid a - qb$. Τότε $d' \mid (a - qb) + qb$, δηλαδή $d' \mid a$.
- $d' \mid a$ και $d' \mid b$ οπότε $d' \mid d$ (διότι $d = (a, b)$).
- Άρα $d = (b, a - qb)$.

Αντίστροφα, εάν ο $(a - qb, b)$ υπάρχει, τότε θα υπάρχει και ο $(a - qb - (-q)b, b)$ δηλαδή θα υπάρχει ο (a, b) και θα είναι ίσοι.
Παραδείγματα:

- $(50, 12) = (50 - 4 \cdot 12, 12) = (2, 12) = (12 - 5 \cdot 2, 2) = (2, 2) = 2$.
- $(10n + 1, 2n) = (10n + 1 - 5 \cdot 2n, 2n) = (1, 2n) = 1$

Ευκλείδιος Αλγόριθμος

Έστω $a, b \in \mathbb{N}$. Ορίζουμε την ακολουθία υπολοίπων r_i: $r_0 = a,\ r_1 = b$ και

$$\begin{aligned} r_0 &= q_1 r_1 + r_2,\ \ 0 < r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3,\ \ 0 < r_3 < r_2 \\ &\vdots \\ r_{\ell-1} &= q_\ell r_\ell + r_{\ell+1},\ \ 0 < r_{\ell+1} < r_\ell \\ r_\ell &= q_{\ell+1} r_{\ell+1} \end{aligned}$$

- Για να υπολογίσουμε το r_i κάνουμε ακέραια διαίρεση του r_{i-2} με το r_{i-1}.
- Η διαδικασία σταματά όταν σε μία διαίρεση βρούμε υπόλοιπο ίσο με 0.
- $r_{\ell+1} = (a, b)$.

Θεώρημα [Ευκλείδιος Αλγόριθμος]

Το τελευταίο μη μηδενικό υπόλοιπο στην παραπάνω ακολουθία είναι ο (a, b).

Η ακολουθία υπολοίπων ικανοποιεί:

$$r_0 = a,\ r_1 = b,\ \ r_{i+2} = r_i - q_{i+1} r_{i+1} \ \text{ για } \ i = 0, \ldots, \ell - 1.$$

Σύμφωνα με την Πρόταση που δείξαμε,

$$(r_i, r_{i+1}) = (r_{i+1}, r_i - q_{i+1} r_{i+1}) = (r_{i+1}, r_{i+2}), \quad \text{για } \ i = 0, \ldots, \ell - 1.$$

Επομένως,

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_\ell, r_{\ell+1}).$$

Όμως $r_\ell = q_{\ell+1} r_{\ell+1}$, οπότε $(r_\ell, r_{\ell+1}) = r_{\ell+1}$ (δείξτε το!)

Θεώρημα ύπαρξης μέγιστου κοινού διαιρέτη

Έστω $a, b \in \mathbb{Z}$, τότε υπάρχει ο μκδ των a, b.

- Εάν $b = 0$, τότε ο $|a|$ είναι μέγιστος κοινός διαιρέτης των a, b.
- Εάν $a = 0$, τότε ο $|b|$ είναι μέγιστος κοινός διαιρέτης των a, b.
- Έαν $a, b \neq 0$, τότε γνωρίζουμε ότι υπάρχει ο $(|a|, |b|)$.
- Ο $(|a|, |b|)$ είναι μέγιστος κοινός διαιρέτης των a, b (δείξτε το!).
- Άρα $(a, b) = (|a|, |b|)$.

Παραδείγματα:

- Θα υπολογίσουμε το $(60, 14)$. Εφαρμόζουμε τον Ευκλείδιο αλγόριθμο:

$$\begin{aligned} 60 &= 4 \cdot 14 + 4 \\ 14 &= 3 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 \end{aligned}$$

  Το τελευταίο μη-μηδενικό υπόλοιπο είναι ο μκδ. Δηλαδή $(60, 14) = 2$.

- Θα υπολογίσουμε το $(n^6 - 1, n^4 - 1)$. Θα χρησιμοποιήσουμε την "Πρόταση $(a, b) = (b, a - qb)$":

$$\begin{aligned} n^6 - 1 &= n^2(n^4 - 1) + n^2 - 1 \\ n^4 - 1 &= (n^2 + 1)(n^2 - 1) \end{aligned}$$

  Άρα $(n^6 - 1, n^4 - 1) = (n^4 - 1, n^2 - 1) = n^2 - 1$.

Πρόταση

Έστω $a, b, n \in \mathbb{N}$. Αν $(a, b) = d$ τότε $(na, nb) = nd$.

Εφαρμόζουμε τον Ευκλείδιο αλγόριθμο για $r_0 = a, r_1 = b$:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2, \ 0 < r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3, \ 0 < r_3 < r_2 \\ &\dots \\ r_{\ell-1} &= q_\ell r_\ell + r_{\ell+1}, \ 0 < r_{\ell+1} < r_\ell \\ r_\ell &= q_{\ell+1} r_{\ell+1} \end{aligned}$$

Οπότε $d = (r_0, r_1) = r_{\ell+1}$. Πολ/ζουμε κάθε ισότητα με n:

$$\begin{aligned} nr_0 &= q_1 nr_1 + nr_2 \\ nr_1 &= q_2 nr_2 + nr_3 \\ &\dots \\ nr_{\ell-1} &= q_\ell nr_\ell + nr_{\ell+1} \\ nr_\ell &= q_{\ell+1} nr_{\ell+1} \end{aligned}$$

Οπότε $(nr_0, nr_1) = (nr_1, nr_2) = \dots = (nr_\ell, nr_{\ell+1}) = nr_{\ell+1} = nd$.

Παραδείγματα:

- Είδαμε ότι $(60, 14) = 2$, άρα

$$(120, 28) = 2 \cdot 2 = 4, \quad (180, 42) = 3 \cdot 2 = 6.$$

- Είδαμε ότι για κάθε $n \in \mathbb{N}$, $(n^6 - 1, n^4 - 1) = n^2 - 1$, άρα

$$(m(n^6 - 1), m(n^4 - 1)) = m(n^2 - 1).$$

Πρόταση

Εάν $d, n, m \in \mathbb{N}$, $d \mid nm$ και $(m, d) = 1$ τότε $d \mid n$.

Βλέπουμε ότι $d \mid nm$ και $d \mid nd$,

- το d είναι κοινός διαιρέτης,
- άρα θα διαιρεί το μέγιστο κοινό διαιρέτη!

$$d \mid (nm, nd) = n(m, d) = n.$$

Πόρισμα

Εάν $n, m \in \mathbb{N}$, p πρώτος αριθμός, $p \mid nm$ και $p \nmid m$ τότε $p \mid n$.

- Ο (m, p) είναι διαιρέτης του p,
- οι μόνοι διαιρέτες του p είναι οι $1, p$,
- αν ήταν $(m, p) = p$, τότε ο p θα διαιρούσε το m,
- αυτό δεν ισχύει, άρα $(m, p) = 1$.
- Το ζητούμενο προκύπτει από την προηγούμενη πρόταση.

Θεώρημα [Θεώρημα Μοναδικής Παραγοντοποίησης]

Κάθε αριθμός $n \in \mathbb{N}$, $n \geq 2$ γράφεται με μοναδικό τρόπο ως γινόμενο πρώτων αριθμών, εάν αγνοήσουμε τη σειρά των παραγόντων. Συγκεκριμένα, εάν $n = p_1 \cdots p_s = q_1 \cdots q_t$, όπου $p_1, \ldots, p_s, q_1, \ldots, q_t$ είναι πρώτοι αριθμοί, τότε $s = t$ και υπάρχει μία αμφιμονοσήμαντη απεικόνιση $\sigma : \{1, \ldots, t\} \longrightarrow \{1, \ldots, t\}$, τέτοια ώστε $p_i = q_{\sigma(i)}$ για κάθε $1 \leq i \leq t$.

Ήδη γνωρίζουμε ότι ο n γράφεται ως γινόμενο πρώτων. Έστω ότι $n = p_1 \cdots p_s = q_1 \cdots q_t$, με $s \leq t$. θα δούμε τη *βασική ιδέα*:

- Ο p_1 διαιρεί τον n, άρα διαιρεί ένα από τους $q_1, \ldots, q_s$. Ας πούμε $p_1 \mid q_{\sigma(1)}$, με $\sigma(1) \in \{1, \ldots, t\}$.
- Τότε $p_1 = q_{\sigma(1)}$ και αφού απλοποιήσουμε έχουμε $\prod_{i \neq 1} p_i = \prod_{j \neq \sigma(1)} q_j$.
- Έχουμε το ίδιο "πρόβλημα" με $s - 1$ πρώτους στο 1ο μέλος και $t - 1$ πρώτους στο 2ο μέλος.
- Συνεχίζουμε με το ίδιο επιχείρημα s συνολικά φορές.
- Έαν $s < t$ τότε στο αριστερό μέλος έχουμε 1 και στο δεξί μέλος ένα γινόμενο πρώτων. Άτοπο!
- Άρα $s = t$ και σε κάθε βήμα κάναμε μία αντιστοίχιση $1 \mapsto \sigma(1), 2 \mapsto \sigma(2), \ldots, s \mapsto \sigma(s)$.

Παράδειγμα: Ας παραγοντοποιήσουμε τον αριθμό 30 σε πρώτους:

- $30 = 2 \cdot 3 \cdot 5 = 3 \cdot 5 \cdot 2$,
- δηλαδή $p_1 = 2, p_2 = 3, p_3 = 5$ και $q_1 = 3, q_2 = 5, q_3 = 2$.
- $p_1 = q_3$, άρα $\sigma(1) = 3$,
- $p_2 = q_1$, άρα $\sigma(2) = 1$,
- $p_3 = q_2$, άρα $\sigma(3) = 2$.

Απόδειξη με επαγωγή στο s:

- Βάση: εάν $s = 1$, τότε $p_1 = q_1 \cdots q_t$. Πρέπει $t = 1$ και $\sigma(1) = 1$.
- Επαγ.Υπόθεση: Η πρόταση ισχύει όταν στο αριστερό μέλος έχουμε s πρώτους.
- Επαγ. Βήμα: Έστω ότι $p_1 \cdots p_s p_{s+1} = q_1 \cdots q_t$. Θα δείξουμε ότι $s + 1 = t$ και υπάρχει αμφιμονοσήμαντη συνάρτηση $\sigma : \{1, \ldots, s+1\} \longrightarrow \{1, \ldots, s+1\}$, τ.ω. $p_i = q_{\sigma(i)}$.
  - Το p_1 διαιρεί το $q_1 \cdots q_t$ άρα $p_1 = q_{i_1}$ και $\prod_{i \neq 1} p_i = \prod_{j \neq i_1} q_j$.
  - Από Ε.Υ. συμπεραίνουμε ότι $s = t - 1$ και υπάρχει αμφιμονοσήμαντη συνάρτηση $\tau : \{2, \ldots, s+1\} \longrightarrow \{1, \ldots, t\} \setminus \{i_1\}$ τ.ω. $p_i = q_{\tau(i)}$, για $2 \leq i \leq s+1$.
  - Άρα $s + 1 = t$. Μένει να βρούμε την αντιστοίχιση σ.
  - Θέτουμε $\sigma(1) = i_1$ και $\sigma(i) = \tau(i)$ για $2 \leq i \leq s+1$.
  - Ισχύει $p_i = q_{\sigma(i)}$ για $1 \leq i \leq s+1$.

Έστω οι ακέραιοι $71, 13$. Υπολογίζω το μκδ τους:

$$\begin{aligned} 71 &= 5 \cdot 13 + 6 \\ 13 &= 2 \cdot 6 + 1 \\ 6 &= 6 \cdot 1 \end{aligned}$$

Ξεκινώ από το τελευταίο μη μηδενικό υπόλοιπο (που είναι ο μκδ):

$$1 = 13 - 2 \cdot 6 = 13 - 2 \cdot (71 - 5 \cdot 13) = (-2) \cdot 71 + 11 \cdot 13.$$

Άρα $(71, 13) = 1 = (-2) \cdot 71 + 11 \cdot 13$.

Έστω οι ακέραιοι $29, 8$. Υπολογίζω το μκδ τους:

$$\begin{aligned} 29 &= 3 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

ξεκινώ από το τελευταίο μη μηδενικό υπόλοιπο (που είναι ο μκδ):

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = (-1) \cdot 5 + 2 \cdot 3 \\ &= (-1) \cdot 5 + 2 \cdot (8 - 5) = 2 \cdot 8 + (-3) \cdot 5 \\ &= 2 \cdot 8 + (-3) \cdot (29 - 3 \cdot 8) = (-3) \cdot 29 + 11 \cdot 8. \end{aligned}$$

Άρα $(29, 8) = 1 = (-3) \cdot 29 + 11 \cdot 8$.

Θεώρημα

Έστω $a, b \in \mathbb{Z}$. Τότε υπάρχουν $s, t \in \mathbb{Z}$ τέτοιοι ώστε $(a, b) = s \cdot a + t \cdot b$.

θυμόμαστε ότι στον Ευκλείδιο αλγόριθμο έχουμε

$$r_0 = a,\ r_1 = b \ \text{ και } \ r_{i+1} = r_{i-1} - q_i r_i, \ \text{ για } 1 \leq i \leq \ell.$$

Θα υπολογίσουμε ακολουθίες s_i, t_i, για $0 \leq i \leq \ell + 1$, τέτοιες ώστε $r_i = s_i \cdot a + t_i \cdot b$.

- $r_0 = a = 1 \cdot a + 0 \cdot b \implies s_0 = 1,\ t_0 = 0.$
- $r_1 = b = 0 \cdot a + 1 \cdot b \implies s_0 = 0,\ t_0 = 1.$
- Ας υποθέσω ότι έχω υπολογίσει τους όρους s_j, t_j, για $0 \leq j \leq i$.
- $$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i \\ &= (s_{i-1} \cdot a + t_{i-1} \cdot b) - q_i \cdot (s_i \cdot a + t_i \cdot b) \\ &= (s_{i-1} - q_i s_i) \cdot a + (t_{i-1} - q_i t_i) \cdot b. \end{aligned}$$
- Άρα θέτω $s_{i+1} = s_{i-1} - q_i s_i$ και $t_{i+1} = t_{i-1} - q_i t_i$.

Τότε $(a, b) = r_{\ell+1} = s_{\ell+1} a + t_{\ell+1} b$. Οι ακέραιοι που ψάχνω είναι οι $s = s_{\ell+1}, t = t_{\ell+1}$.