Υπολογιστικά & Διακριτά Μαθηματικά

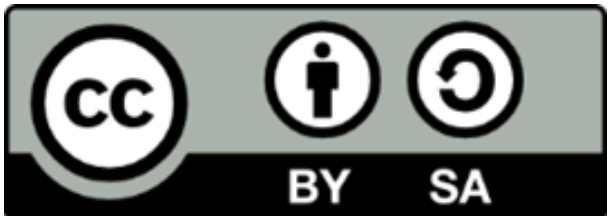
Ενότητα 10: Αριθμητική υπολοίπων - Κυκλικές ομάδες: Διαιρετότητα - Ευκλείδειος αλγόριθμος - Κατάλοιπα

Στεφανίδης Γεώργιος

Τμήμα Εφαρμοσμένης Πληροφορικής

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Διαιρετότητα [1]

- Έστω $a, b, d \in \mathbb{Z}$. Τότε

1. Ο a **διαιρεί** τον b, συμβολικά $a \mid b$, αν υπάρχει $c \in \mathbb{Z}$ με $b = ac$. Αν $a \mid b$, τότε λέμε και ότι ο b είναι **πολλαπλάσιο** του a. Αν τώρα ο a δεν διαιρεί τον b, γράφουμε $a \nmid b$.
2. Αν $d \mid a$ και $d \geq 0$, ο d λέγεται **διαιρέτης** του a. Κάθε ακέραιος a έχει σαν *τετριμμένους διαιρέτες* τους 1 και a. Οι μη τετριμμένοι διαιρέτες του a λέγονται και *παράγοντες* του a.
   - Ένας ακέραιος $a > 1$ του οποίου οι μόνοι διαιρέτες είναι οι τετριμμένοι διαιρέτες 1 και a λέγεται ότι είναι *πρώτος αριθμός* ή απλά *πρώτος*.
   - Αποδεικνύεται ότι *υπάρχουν άπειροι πρώτοι*.
   - Ένας ακέραιος $a > 1$ ο οποίος δεν είναι πρώτος λέγεται ότι είναι *σύνθετος αριθμός* ή απλά *σύνθετος*. Ο ακέραιος 1 δεν είναι πρώτος ούτε σύνθετος. Παρόμοια, ο ακέραιος 0 και όλοι οι αρνητικοί ακέραιοι δεν είναι ούτε πρώτοι ούτε σύνθετοι.
3. Αν p είναι πρώτος και $p \mid ab$, $a, b \in \mathbb{N}$, τότε $p \mid a$ ή $p \mid b$.
4. Ο $d \in \mathbb{N}$ λέγεται μέγιστος κοινός διαιρέτης των a και b, συμβολικά $\gcd(a, b)$, αν:
   - $d \mid a$ και $d \mid b$.
   - αν $t \in \mathbb{Z}$ διαιρεί τον a και b, τότε διαιρεί τον d.
5. Αν $\gcd(a, b) = 1$, τότε ο a λέγεται *σχετικά πρώτος* με τον b, ή ότι οι a και b είναι *πρώτοι μεταξύ τους* ή ότι οι a και b είναι *σχετικά πρώτοι*.

Διαιρετότητα [2]

❑ **Θεώρημα 1** (Διαίρεση με υπόλοιπο)

Έστω $z, a \in \mathbb{Z}, a \neq 0$. Τότε υπάρχουν μοναδικοί ακέραιοι $q, r \in \mathbb{Z}$, τέτοιοι, ώστε $z = q \cdot a + r$ και $0 \leq r < |a|$.

- Ο r λέγεται **υπόλοιπο** του z modulo a (δηλ. $r := \boldsymbol{z \bmod a}$).
- Ο αριθμός q είναι το (ακέραιο) *πηλίκο* των z και a, συμβολικά z div a (δηλ. $q := z$ div a) και είναι $q = \lfloor z/a \rfloor$, όπου $\lfloor x \rfloor$ είναι ο μεγαλύτερος ακέραιος που δεν υπερβαίνει τον αριθμό x. Επίσης
  - $a \mid z \Leftrightarrow z \bmod a = 0$.

❑ **Θεώρημα 2**

Ένας σύνθετος a μπορεί να γραφεί κατά μοναδικό τρόπο ως γινόμενο της μορφής

$$\boldsymbol{a = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} = \prod_{i=1}^{s} p_i^{e_i}}$$

Αλγόριθμος του Ευκλείδη [1]

- Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $a \geq b \geq 0$.
  - Αν $b = 0$, τότε $\gcd(a, 0) = a$.
  - Αν $b > 0$, μπορούμε να υπολογίσουμε το ακέραιο πηλίκο $q := \lfloor a/b \rfloor$ και το υπόλοιπο $r := a \bmod b$, όπου $0 \leq r < b$.
  - Από την εξίσωση $a = bq + r$ είναι εύκολο να συμπεράνουμε ότι
    - $\gcd(a, b) = \gcd(b, r)$

    και έτσι, εκτελώντας μία διαίρεση, υποβιβάζουμε το πρόβλημα του υπολογισμού του $\gcd(a, b)$ στο "μικρότερο" πρόβλημα του υπολογισμού του $\gcd(b, r)$.
- Παραδείγματος χάριν,

$$\begin{aligned} \gcd(100, 35) &= \gcd(35, 100 \bmod 35) = \gcd(35, 30) \\ &= \gcd(30, 35 \bmod 30) = \gcd(30, 5) \\ &= \gcd(5, 30 \bmod 5) = \gcd(5, 0) \\ &= 5. \end{aligned}$$

Αλγόριθμος του Ευκλείδη [2]

❑ **Θεώρημα 3**

Έστω ότι οι a, b είναι ακέραιοι, με $a \geq b \geq 0$. Χρησιμοποιώντας τη διαίρεση με υπόλοιπο, ορίζουμε της ακεραίους $r_0, r_1, \ldots, r_{l+1}$ και $q_1, \ldots, q_\ell$, όπου $\ell \geq 0$, ως εξής:

$a = r_0$,

$b = r_1$,

$r_0 = r_1 q_1 + r_2 \quad (0 < r_2 < r_1)$,

...

$r_{i-1} = r_i q_i + r_{i+1} \quad (0 < r_{i+1} < r_i)$,

...

$r_{\ell-2} = r_{\ell-1} q_{\ell-1} + r_\ell \quad (0 < r_\ell < r_{\ell-1})$,

$r_{\ell-1} = r_\ell q_\ell \quad (r_{\ell+1} = 0)$.

❖ Να σημειωθεί ότι, εξ ορισμού, $\ell = 0$ αν $b = 0$, και $\ell > 0$, διαφορετικά.

➢ Τότε έχουμε $r_\ell = \gcd(a, b)$.

Αλγόριθμος του Ευκλείδη [3]

- **Παράδειγμα 1**
- Έστω $a = 3094$ και $b = 2513$. Έχουμε $r_0 = a = 3094$, $r_1 = b = 2513$, και $q_i = \lfloor r_{i-1}/r_i \rfloor$, $r_{i+1} = r_{i-1} - r_i q_i$ για $i = 1, 2, \ldots$. Τότε οι αριθμοί που εμφανίζονται στο παραπάνω θεώρημα υπολογίζονται εύκολα ως εξής:

i	0	1	2	3	4	5	6
r_i	3094	2513	581	189	14	7	0
q_i		1	4	3	13	2	

➢ Έτσι έχουμε, gcd(3094, 2513) = $r_5 = 7$.

- Μπορούμε εύκολα να μετατρέψουμε το σχήμα που περιγράφεται στο Θεώρημα 3 σε έναν απλό αλγόριθμο:

❑ **Αλγόριθμος *Ευκλείδειος Επαναληπτικός*(*a*, *b*)**

r ← a, r′ ← b

while r′ ≠ 0

$r'' \leftarrow r \bmod r'$

$(r, r') \leftarrow (r', r'')$

$d \leftarrow r$

return d

Διευρυμένος Αλγόριθμος του Ευκλείδη [1]

- Έστω ότι οι a και b είναι μη αρνητικοί ακέραιοι και έστω $d := \gcd(a, b)$. Ξέρουμε από σχετικό θεώρημα της θεωρίας αριθμών ότι υπάρχουν ακέραιοι s και t, τέτοιοι, ώστε $as + bt = d$. Ο διευρυμένος Ευκλείδειος αλγόριθμος μας επιτρέπει να υπολογίσουμε αποδοτικά τους s και t. Στηρίζεται στο γεγονός ότι μπορούμε να γράψουμε κάθε υπόλοιπο r_i κατά τη διαδικασία υπολογισμού του $\gcd(a, b)$.
- Για παράδειγμα, έστω ότι έχουμε τους ακεραίους $a = 1281$ και $b = 243$. Εκτελούμε τους υπολογισμούς για τον μκδ και παραπλεύρως τους υπολογισμούς για τους s και t.
- $1281 = 243 \cdot 5 + 66 \Rightarrow 66 = 1281 - 243 \cdot 5$
- $243 = 66 \cdot 3 + 45 \Rightarrow 45 = 243 - 66 \cdot 3 = 243 - 3(1281 - 243 \cdot 5) = 16 \cdot 243 - 3 \cdot 1281$
- $66 = 45 \cdot 1 + 21 \Rightarrow 21 = 66 - 45 \cdot 1 = 1281 - 243 \cdot 5 - 16 \cdot 243 + 3 \cdot 1281$
  $= 4 \cdot 1281 - 21 \cdot 243$
- $45 = 21 \cdot 2 + 3 \Rightarrow 3 = 45 - 21 \cdot 2 = 16 \cdot 243 - 3 \cdot 1281 - 2(4 \cdot 1281 - 21 \cdot 243)$
  $= -11 \cdot 1281 + 58 \cdot 243 = -11a + 58b$
- $21 = 3 \cdot 7 + 0$
  $\Rightarrow \gcd(1281, 243) = (-11) \cdot 1281 + 58 \cdot 243.$

Θεώρημα 4

❑ Θεώρημα 4

- Έστω οι $a, b, r_0, r_1, \ldots, r_{\ell+1}$ και $q_1, \ldots, q_\ell$, όπως στο Θεώρημα 3. Ορίζουμε ακεραίους $s_0, s_1, \ldots, s_{\ell+1}$ και $t_0, t_1, \ldots, t_{\ell+1}$ ως εξής:
  - $s_0 := 1, \quad t_0 := 0,$
  - $s_1 := 0, \quad t_1 := 1,$

  και για $i = 1, \ldots, \ell$,
  - $s_{i+1} := s_{i-1} - s_i q_i, \quad t_{i+1} := t_{i-1} - t_i q_i .$

➢ Τότε

για $i = 0, \ldots, \ell + 1$, έχουμε $s_i a + t_i b = r_i$. Ειδικότερα, $s_\ell a + t_\ell b = \gcd(a, b)$.

❖ *Παρατήρηση*. Τα r_i είναι όπως στον Ευκλείδειο αλγόριθμο. Τα s_i, t_i "αρχικοποιούνται" και υπολογίζονται με τους παραπάνω τύπους. Πρόκειται για τύπους με το ίδιο πρότυπο:

- $x_{i+1} = x_{i-1} - q_i x_i$ όπου $q_i = \lfloor r_{i-1} / r_i \rfloor$.

Διευρυμένος Αλγόριθμος του Ευκλείδη [2]

- **Παράδειγμα 2**

Επεκτείνουμε το Παράδειγμα 1. Οι αριθμοί s_i και t_i υπολογίζονται εύκολα από το q_i:

i	0	1	2	3	4	5	6
r_i	3094	2513	581	189	14	7	0
q_i		1	4	3	13	2	
s_i	1	0	1	–4	13	–173	359
t_i	0	1	–1	5	–16	213	–442

➢ Έτσι έχουμε, $\gcd(a, b) = 7 = -173a + 213b$.

Διευρυμένος Αλγόριθμος του Ευκλείδη [3]

- Μπορούμε εύκολα να μετατρέψουμε το σχήμα που περιγράφεται στο Θεώρημα 4 σε έναν επαναληπτικό αλγόριθμο:
- Αλγόριθμος *ΕυκλείδειοςΔιευρυμένοςΕπαναληπτικός*(*a*, *b*)

$r \leftarrow a, r' \leftarrow b$

$s \leftarrow 1, s' \leftarrow 0$

$t \leftarrow 0, t' \leftarrow 1$

while $r' \neq 0$

$$q \leftarrow \lfloor r/r' \rfloor, \quad r'' \leftarrow r \bmod r'$$

$$(r, s, t, r', s', t') \leftarrow (r', s', t', r'', s - s'q, t - t'q)$$

$d \leftarrow r$

return d, s, t

Κατάλοιπα [1]

- Συνοψίζοντας όσα είπαμε και σε προηγούμενο μάθημα για την ισοτιμία "$\equiv \pmod n$" δίνουμε τον ακόλουθο ορισμό.
- Έστω $n \in \mathbb{N}$, $n \geq 2$:

1. Οι $a, b \in \mathbb{Z}$ είναι *ισότιμοι modulo n*, συμβολικά $a \equiv b \pmod n$, αν $n \mid a - b$.
2. Έστω $a \in \mathbb{Z}$. Το σύνολο

$$[a] := \{x \in \mathbb{Z} : x \equiv a \pmod n\} = \{x : x = a + kn, k \in \mathbb{Z}\}$$

λέγεται *κλάση καταλοίπων* του a modulo n.

3. Το $\mathbb{Z}_n := \{[a] : a \in \mathbb{Z}\}$ είναι το σύνολο των κλάσεων καταλοίπων modulo n.

- Το σημείο (1) του παραπάνω ορισμού σημαίνει ότι οι a και b έχουν το ίδιο υπόλοιπο όταν διαιρεθούν με τον n:

$$a \equiv b \pmod n \Leftrightarrow a \bmod n = b \bmod n.$$

- Σε σχέση με το σημείο 2, σε προηγούμενο μάθημα είδαμε ότι "ισότιμοι modulo n" είναι μια σχέση ανακλαστική, συμμετρική και μεταβατική, δηλ. είναι μια σχέση ισοδυναμίας:
  - $a \equiv a \pmod n$
  - $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$
  - ($a \equiv b \pmod n$ και $b \equiv c \pmod n$) $\Rightarrow a \equiv c \pmod n$.

Κατάλοιπα [2]

- Οι κλάσεις καταλοίπων είναι οι κλάσεις ισοδυναμίας. Συνεπώς σύμφωνα με όσα ξέρουμε για της κλάσεις ισοδυναμίας, είναι

$$a \equiv b \pmod{n} \Leftrightarrow [a] = [b]$$

- Μια κλάση καταλοίπων $[a]$ προσδιορίζεται πλήρως από ένα εκ των μελών της. Αν $a' \in [a]$, τότε $[a] = [a']$. Ένα στοιχείο $x \in [a]$ λέγεται *αντιπρόσωπος* της κλάσης $[a]$. Ισχύει ότι

$$a \equiv a \bmod n \pmod{n} \quad (\text{δηλ. } [a] = [a \bmod n])$$

  - Πράγματι, είναι

$$a = qn + r,\ 0 \le r < n \ \Rightarrow\ a - r = qn \ \Rightarrow\ n \mid a - r \ \Rightarrow\ a \equiv r \pmod{n} \ (\Rightarrow [a] = [r])$$

- Για το σημείο 3, να πούμε ότι η διαίρεση με το n δίνει τα υπόλοιπα $0, \ldots, n-1$. Επομένως, υπάρχουν n το πολύ κλάσεις καταλοίπων στο $\mathbb{Z}_n$:

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

- Οι ακέραιοι $0, \ldots, n-1$ λέγονται *φυσικοί αντιπρόσωποι*. Ο φυσικός αντιπρόσωπος της κλάσης $[x]$ είναι απλώς το υπόλοιπο ($x \bmod n$) του x modulo n (βλ. διαίρεση με υπόλοιπο). Αν στα δεδομένα πλαίσια, δεν είναι δυνατό να δημιουργηθεί σύγχυση, «ταυτίζουμε» τις κλάσεις καταλοίπων με τους φυσικούς αντιπροσώπους της. Καλούμε το $x \bmod n$ και ως το *μικρότερο μη αρνητικό κατάλοιπο* του x modulo n. Επίσης λέμε ότι το $x \bmod n$ είναι το αποτέλεσμα της αναγωγής του x modulo n.

Θεώρημα 5 [1]

- **Θεώρημα 5**

Έστω $a, b, c, d \in \mathbb{Z}$ και $f(x)$ ένα πολυώνυμο με ακέραιους συντελεστές. Αν

$$a \equiv b \pmod{n} \text{ και } c \equiv d \pmod{n},$$

τότε

α) $a + c \equiv b + d \pmod{n}$

β) $a \cdot c \equiv b \cdot d \pmod{n}$

γ) $a^k \equiv b^k \pmod{n}$, $k \in \mathbb{N}$

δ) $f(a) \equiv f(b) \pmod{n}$.

- **Παράδειγμα 3**

- Αν $a, b \in \mathbb{Z}$ και p πρώτος, τότε

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

Απόδειξη

- Είναι, όπως ξέρουμε $\boldsymbol{(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k}$
- και για $k = 1, \ldots, p-1$ έχουμε $\boldsymbol{\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}}$

Θεώρημα 5 [2]

- οπότε $p(p-1)\cdots(p-k+1) = k!\binom{p}{k}$
- Επομένως $p \mid k!\binom{p}{k}$

και επειδή gcd(p, k!) = 1, διότι p είναι πρώτος και k! = 1·2 k, παίρνουμε ότι $p \mid \binom{p}{k}$

❖ (Είναι γνωστή πρόταση της θεωρίας αριθμών: Αν p είναι πρώτος, $p \mid ab$, και gcd(p, b) = 1, όπου $a, b \in \mathbb{Z}$, τότε $p \mid a$.)

- Άρα, για $k = 1, \ldots, p-1$ $\binom{p}{k} \equiv 0 \pmod{p}$

- και συνεπώς $(a+b)^p \equiv a^{p-0}b^0 + a^{p-p}b^p \equiv a^p + b^p \pmod{p}$

Θεώρημα 5 [3]

- Μια ομάδα $(G, *)$ είναι *πεπερασμένη* αν το σύνολο G έχει πεπερασμένο πλήθος στοιχείων, δηλ. αν είναι πεπερασμένος ο πληθικός αριθμός $|G|$. Σ' αυτή την περίπτωση ο αριθμός $|G|$ λέγεται *τάξη* της ομάδας. Αν το G δεν είναι πεπερασμένο τότε λέμε ότι η ομάδα είναι *απείρου* τάξης.
- Στο σύνολο $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ των κλάσεων ισοδυναμίας, είναι εύκολο να δούμε ότι η κλάση ισοδυναμίας δύο ακεραίων προσδιορίζει μονοσήμαντα την κλάση ισοδυναμίας του αθροίσματος ή του γινομένου τους. Με άλλα λόγια,
- αν $a \equiv a' \pmod{n}$ και $b \equiv b' \pmod{n}$,
- τότε
- $a + b \equiv a' + b' \pmod{n}$ και $a \cdot b \equiv a' \cdot b' \pmod{n}$.

Θεώρημα 5 [4]

- Έτσι, ορίζουμε πρόσθεση και πολλαπλασιασμό modulo n, συμβολικά $+_n$ και $\cdot_n$ ως ακολούθως:

$$[a] +_n [b] = [a + b] \quad \text{και} \quad [a] \cdot_n [b] = [a \cdot b]$$

- Μπορούμε να δούμε τις παραπάνω πράξεις ως εξής
- $+ : (a, b) \rightarrow a + b \bmod n$
- $\cdot \ : (a, b) \rightarrow a \cdot b \bmod n$
- Δηλαδή, η πρόσθεση και ο πολλαπλασιασμός εκτελούνται, κατά τον συνήθη τρόπο, επί των αντιπροσώπων, αλλά το κάθε αποτέλεσμα x αντικαθίσταται με τον αντιπρόσωπο της κλάσης του, δηλ. με $x \bmod n$ (που είναι το υπόλοιπο της διαίρεσης του x με το n — αναγωγή του x modulo n).

Τέλος Ενότητας

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης