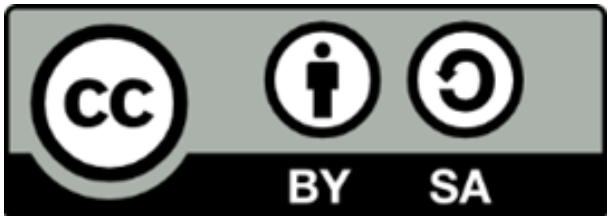
Υπολογιστικά & Διακριτά Μαθηματικά

Ενότητα 12: Κυκλικές ομάδες – Κινέζικο Θεώρημα Υπολοίπων

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.

Δυαδική εκθετοποίηση a^n [1]

- Έστω $n = b_\ell \ldots b_i \ldots b_0$ η δυαδική συμβολοσειρά που αναπαριστά τον θετικό ακέραιο n. Αυτό σημαίνει ότι η τιμή του n μπορεί να υπολογιστεί ως η τιμή του πολυωνύμου

$$p(x) = b_\ell x^\ell + \cdots + b_i x^i + \cdots + b_0 x^0$$

στο $x = 2$.

- Π. χ. αν $n = 13$, η δυαδική αναπαράστασή του είναι 1101 αφού

$$13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

Δυαδική εκθετοποίηση a^n [2]

- Ας υπολογίσουμε την τιμή του πολυωνύμου $p(x)$ εφαρμόζοντας τον κανόνα του Horner και ας δούμε πως μεταφέρονται οι υπολογισμοί στην περίπτωση υπολογισμού της δύναμης

$$a^n = a^{p(2)} = a^{b_\ell 2^\ell + \cdots + b_i 2^i + \cdots + b_0 2^0}$$

Κανόνας του Horner για το πολυώνυμο $p(2)$

$p \leftarrow 1$ // ο μεγιστοβάθμιος συντελεστής
// είναι πάντα 1 για $n \geq 1$

for $i \leftarrow \ell - 1$ **downto** 0

$p \leftarrow 2p + b_i$

Εφαρμογή στον υπολογισμό της $a^n = a^{p(2)}$

$a^p \leftarrow a^1$

for $i \leftarrow \ell - 1$ **downto** 0

$a^p \leftarrow a^{2p+b_i}$

Δυαδική εκθετοποίηση a^n [3]

- Επειδή
$$a^{2p+b_i} = a^{2p} \cdot a^{b_i} = (a^p)^2 \cdot a^{b_i} = \begin{cases} (a^p)^2, & \text{αν } b_i = 0 \\ (a^p)^2 \cdot a, & \text{αν } b_i = 1 \end{cases}$$
- οδηγούμαστε στον ακόλουθο αλγόριθμο
- **Αλγόριθμος** *ΔυαδικήΕκθετοποίηση*(*a*, *b*(*n*))
- // Υπολογίζει τη δύναμη a^n με ύψωση από αριστερά προς τα δεξιά στη // δυαδική αναπαράσταση
- // Είσοδος: Ένας αριθμός *a* και μια λίστα *b*(*n*) δυαδικών ψηφίων $b_\ell, \ldots, b_0$ στο
- // δυαδικό ανάπτυγμα ενός θετικού ακεραίου *n*
- // Έξοδος: Η τιμή της δύναμης a^n

product ← *a*
for *i* ← ℓ – 1 **downto** 0

product ← product * product

if $b_i = 1$ product ← product * *a*

return product

Παράδειγμα [1]

- Παράδειγμα: Ας δούμε πώς εκτελεί ο παραπάνω αλγόριθμος τον υπολογισμό της δύναμης a^{13}
- Είναι $n = 13 = 1101_2$, οπότε έχουμε

i	3	2	1	0
b_i	1	1	0	1
	a	$a^2 \cdot a$	$(a^3)^2$	$(a^6)^2 \cdot a$
		$= a^3$	$= a^6$	$= a^{13}$

- Αν τώρα θέλουμε να υπολογίσουμε τη δύναμη a^n mod m, τότε παίρνουμε το υπόλοιπο modulo m μετά από κάθε τετραγωνισμό και πολλαπλασιασμό. Μπορούμε λοιπόν να γράψουμε τον αλγόριθμο *ΔυαδικήΕκθετοποίηση*(a, b(n)) ως εξής:
- **Αλγόριθμος** *ΜοdΔυαδικήΕκθετοποίηση*(a, b(n))
- product $\leftarrow a$
- **for** $i \leftarrow \ell - 1$ **downto** 0

$$\begin{cases} \text{product} \leftarrow \text{product} * \text{product} \mod m \\ \text{if } b_i = 1 \quad \text{product} \leftarrow \text{product} * a \mod m \end{cases}$$

- **return** product

Παράδειγμα [2]

- Ας υπολογίσουμε τη δύναμη 17^{22} mod 21.
- Είναι $22 = 10110_2$ οπότε έχουμε με τον αλγόριθμο εκθετοποίησης τον ακόλουθο πίνακα τον οποίο συμπληρώνουμε από αριστερά στα δεξιά:

i	4	3	2	1	0
b_i	1	0	1	1	0
	$17 \bmod 21 = 17$	$17^2 \bmod 21 = 16$	$(16)^2 \cdot 17 \bmod 21 = 5$	$(5)^2 \cdot 17 \bmod 21 = 5$	$(5)^2 \bmod 21 = 4$

➢ Άρα, $17^{22} \bmod 21 = 4$.

Κυκλικές ομάδες

❑ Θεώρημα

- Αν G είναι μια πεπερασμένη ομάδα και $a \in G$, τότε $a^{(|G|)} = e$.

➢ **Εφαρμογή 1**. *Fermat*:

$$\left.\begin{array}{c} p \text{ πρώτος} \\ a \in \mathbb{Z} \\ \gcd(a,p)=1 \end{array}\right\} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

✓ διότι αν $G = \mathbb{Z}_p^*$ με $|G| = |\mathbb{Z}_p^*| = p - 1$, τότε $[a]^{p-1} = 1$.

➢ **Εφαρμογή 2**. *Euler*:

$$\left.\begin{array}{c} n \in \mathbb{N} \\ a \in \mathbb{Z} \\ \gcd(a,n)=1 \end{array}\right\} \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

✓ διότι αν $G = \mathbb{Z}_n^*$ με $|G| = |\mathbb{Z}_n^*| = \phi(n)$, τότε $[a]^{\phi(n)} = 1$.

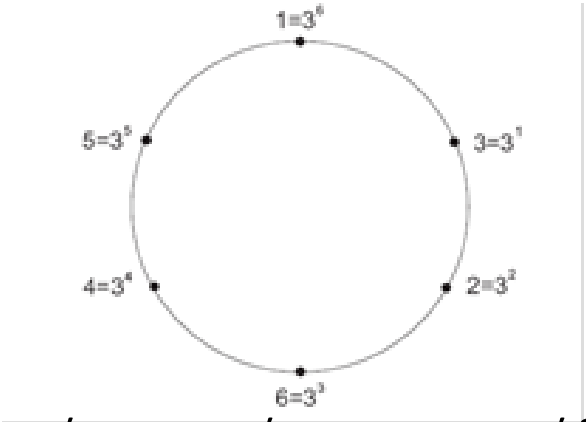
- Έστω τώρα G μια πεπερασμένη ομάδα. Η ομάδα G λέγεται **κυκλική** αν υπάρχει $a \in G$ το οποίο παράγει το G, δηλ. $G = \{a, a^{(2)}, \ldots, a^{(\text{ord}(a)-1)}, a^{(\text{ord}(a))} = e\} = \langle \alpha \rangle$. Ένα τέτοιο στοιχείο a λέγεται ότι είναι ένας **γεννήτορας** της G.

Παράδειγμα [3]

- Παράδειγμα: Στην πολλαπλασιαστική ομάδα $\mathbb{Z}_7^*$ αν βρούμε τις δυνάμεις των στοιχείων της θα έχουμε

k	1	2	3	4	5	6
$1^k \bmod 7$	1	1	1	1	1	1
$2^k \bmod 7$	2	4	1	2	4	1
$3^k \bmod 7$	3	2	6	4	5	1
$4^k \bmod 7$	4	2	1	4	2	1
$5^k \bmod 7$	5	4	6	2	3	1
$6^k \bmod 7$	6	1	6	1	6	1

- Συνεπώς είναι μια κυκλική ομάδα με γεννήτορα το 3, δηλ. $\mathbb{Z}_7^* = \langle 3 \rangle$. Αυτό σημαίνει ότι κάθε στοιχείο του $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ μπορεί να αναπαρασταθεί ως δύναμη του 3



- Στο παράδειγμά μας το 5 είναι επίσης γεννήτορας της ομάδας, δηλ. $\mathbb{Z}_7^* = \langle 5 \rangle$.

Άσκηση

1. Ποιο είναι το υπόλοιπο της διαίρεσης $2^{37} : 7$;
2. Ποιο είναι το υπόλοιπο της διαίρεσης $(4^{10} \cdot 7^7) : 5$;

- ***Λύση***

1. Είναι $2^1 = 2 \equiv 2 \pmod 7$
   $2^2 = 4 \equiv 4 \pmod 7$
   $2^3 = 8 \equiv 1 \pmod 7$
   και $37 = 3 \cdot 12 + 1$.
   - Άρα, $2^{37} = 2^{3 \cdot 12+1} = (2^3)^{12} \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod 7$. Επομένως το ζητούμενο υπόλοιπο είναι 2.
2. Είναι $4^1 = 4 \equiv 4 \pmod 5$
   $4^2 = 16 \equiv 1 \pmod 5$
   και $10 = 2 \cdot 5$.
   - Άρα $4^{10} = (4^2)^5 \equiv 1^5 \pmod 5$.

   Επίσης
   - $7 \equiv 2 \pmod 5 \Rightarrow 7^7 \equiv 2^7 \pmod 5$
   - $2^1 \equiv 2 \pmod 5$
   - $2^2 \equiv 4 \pmod 5$
   - $2^3 \equiv 3 \pmod 5$
   - $2^4 \equiv 1 \pmod 5$
   - και $7 = 4 \cdot 1 + 3$
   - οπότε $2^7 = 2^{4 \cdot 1+3} = (2^4)^{1+3} = (2^4)^1 \cdot 2^3 \equiv 1 \cdot 3 \equiv 3 \pmod 5$.
   - Τελικά
   - $4^{10} \cdot 7^7 \equiv 1 \cdot 3 \equiv 3 \pmod 5$.
   - Επομένως το ζητούμενο υπόλοιπο είναι 3.

Ομομορφισμός – Ισομορφισμός [1]

- Σημαντικό ρόλο στη σύγκριση δύο αλγεβρικών δομών παίζουν, όπως έχουμε αναφέρει ήδη, οι απεικονίσεις μεταξύ ομάδων που διατηρούν τις πράξεις. Ας δώσουμε ορισμένους ορισμούς τέτοιων απεικονίσεων.
- Αν $(G, \circ)$ και $(H, *)$ είναι ομάδες και $f : G \to H$ είναι μια απεικόνιση της ομάδας G στην ομάδα H που διατηρεί την πράξη της G, δηλαδή είναι τέτοια, ώστε

$$\forall\, a, b \in G,\ f(a \circ b) = f(a) * f(b),$$

τότε η f λέγεται ***ομοιομορφισμός*** ή ***ομομορφισμός*** της G στην H.

- Αν η f είναι ένας ένα-προς-ένα ομοιομορφισμός της G *επί* της H τότε λέμε ότι η f είναι ένας ***ισομορφισμός*** και ότι οι ομάδες G και H είναι ***ισομορφικές***, συμβολικά $(G, \circ) \cong (H, *)$ ή απλά $G \cong H$. Εννοείται ότι αν η f είναι ένας ισομορφισμός το ίδιο θα είναι και η f^{-1}.
- Ας θεωρήσουμε, για παράδειγμα, την απεικόνιση f της προσθετικής ομάδας $\mathbb{Z}$ των ακεραίων επί της ομάδας $\mathbb{Z}_n$ των ακεραίων modulo n, που ορίζεται από την $f(a) = [a]$. Τότε

$$f(a + b) = [a + b] = [a] + [b] = f(a) + f(b), \quad \text{για } a, b \in \mathbb{Z},$$

δηλαδή η f είναι ένας ομοιομορφισμός.

- Δύο απλά παραδείγματα ισομορφισμών είναι τα εξής:

Ομομορφισμός – Ισομορφισμός [2]

1. $f : (\{1, -1, i, -i\}, \cdot) \rightarrow (\mathbb{Z}_4, +)$

   Είναι $\{1, -1, i, -i\} = < i >$ με $f(i^n) = [n]_4$ (ή απλά $f(i^n) = n$)

2. $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+, \cdot)$ με $f(x) = e^x$

   $\leftarrow$ με $f^{-1}(x) = \ln x$

- Ισομορφισμός σημαίνει γενικότερα ότι το πεδίο ορισμού και το σύνολο τιμών της f μπορούν να θεωρηθούν ίδια σε ότι αφορά τις πράξεις των ομάδων. Είναι εύκολο να αποδείξει κανείς την

❑ ***Πρόταση***

Μια κυκλική ομάδα τάξεως n είναι ισομορφική με την $\mathbb{Z}_n$.

- Έτσι, αν ξέρουμε την $\mathbb{Z}_n$ τότε ξέρουμε όλες τις δομικές ιδιότητες της οποιασδήποτε κυκλικής ομάδας τάξεως n.
- Η ομάδα $\mathbb{Z}_p^*$ είναι κυκλική για κάθε πρώτο αριθμό p και αυτή η ομάδα είναι ισομορφική με την $\mathbb{Z}_{p-1}$, αφού είναι τάξεως $p-1$.
- Παραδείγματος χάρη, η συνάρτηση $f(x) = g^x \bmod p$ ορίζει έναν ισομορφισμό μεταξύ των $\mathbb{Z}_{p-1}$ και $\mathbb{Z}_p^*$.
- Αυτός ο ισομορφισμός αντανακλάται από την εξίσωση

$$g^{x+y} = g^x \cdot g^y$$

Ομομορφισμός – Ισομορφισμός [3]

- Μια απεικόνιση ρ από έναν δακτύλιο R σε έναν δακτύλιο R' καλείται ***ομομορφισμός δακτυλίων*** αν είναι ομομορφισμός ομάδων ως προς τις αντίστοιχες προσθετικές ομάδες των R και R' και αν επιπλέον,

  1. $\rho(ab) = \rho(a)\rho(b)$ για κάθε $a, b \in R$, και
  2. $\rho(1_R) = 1_{R'}$.

- Επεκτείνοντας τον ορισμό βλέπουμε ότι οι προϋποθέσεις που η απεικόνιση ρ πρέπει να ικανοποιεί για να είναι ομοιομορφισμός δακτυλίων είναι ότι,

  για κάθε $a, b \in R$,

  $$\rho(a + b) = \rho(a) + \rho(b),\ \rho(ab) = \rho(a) \cdot \rho(b) \text{ και } \rho(1_R) = 1_{R'}$$

- Αν ένας ομοιομορφισμός δακτυλίων $\rho : R \to R'$ είναι μια αμφιμονοσήμαντη αντιστοιχία, τότε καλείται ***ισομορφισμός δακτυλίων*** του R με τον R'. Αν ένας τέτοιος ισομορφισμός δακτυλίων ρ υπάρχει, λέμε ότι ο δακτύλιος R *είναι* ***ισομορφικός*** *με τον* R' και γράφουμε $R \cong R'$.

- Αν $f : R \to R'$ είναι ένας ισομορφισμός πεπερασμένων δακτυλίων, οι πίνακες της πρόσθεσης και του πολλαπλασιασμού του R' θα είναι οι ίδιοι με εκείνους του R αν αντικαταστήσουμε κάθε $a \in R$ με $f(a) \in R'$.

Κινέζικο Θεώρημα Υπολοίπων

- Βλέπε: **Σημειώσεις**

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