No. Date 28.3.15

Εφαρμοσμένη Άλγεβρα (Φροντιστήριο 20)

Άσκηση 1 (Εργασία Άσκηση 2)

Να βρεθεί η μήτρα A^n για κάθε $n \in \mathbb{N}^*$, όπου

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Θα προσπαθήσουμε να "μαντέψουμε" την απάντηση και στη συνέχεια θα αποδείξουμε τον ισχυρισμό μας.

$$A^2 = A \cdot A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$A^3 = A \cdot A^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$$

$$A^4 = A \cdot A^3 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}$$

Εικάζουμε ότι $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$

Θα αποδείξουμε την εικασία μας με επαγωγή ως προς n.

Για $n=1$ έχουμε $A^1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = A$, άρα για $n=1$ ισχύει ο ισχυρισμός

Έστω ότι ισχύει για $n=k$, δηλαδή $A^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$

Θα δείξουμε ότι ο τύπος ισχύει για $n=k+1$.

$$A^{k+1} = A \cdot A^k = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1\cdot 1+1\cdot 0 & 1\cdot k+1\cdot 1 \\ 0\cdot 1+1\cdot 0 & 0\cdot k+1\cdot 1 \end{bmatrix} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}$$

Άρα, ο τύπος επαληθεύεται και για $n=k+1$, δηλαδή ισχύει για κάθε $n \in \mathbb{N}^*$.

No. Date

Άσκηση 2

Να βρεθεί η αντίστροφη της μήτρας A (αν υπάρχει) όπου

$$A = \begin{bmatrix} 1 & a & 3 \\ -2 & b & a \\ 0 & 1 & 2 \end{bmatrix} \quad a, b \in \mathbb{R}$$

Θεωρούμε τις μήτρες $A | I_3$. Θα μετασχηματίσουμε την A σε ανηγμένη κλιμακωτή μήτρα και ταυτόχρονα θα εφαρμόσουμε τους ίδιους μετασχηματισμούς στη μήτρα I_3. Στο τέλος, αν η A είναι ανηγμένη κλιμακωτή η I_3 θα έχει μετασχηματιστεί στην A^{-1}.

$$\left[\begin{array}{ccc|ccc} 1 & a & 3 & 1 & 0 & 0 \\ -2 & b & a & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 \end{array}\right] \xrightarrow{R_2 \to R_2 + 2R_1} \left[\begin{array}{ccc|ccc} 1 & a & 3 & 1 & 0 & 0 \\ 0 & b+2a & a+6 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 \end{array}\right] \xrightarrow{R_2 \leftrightarrow R_3} \left[\begin{array}{ccc|ccc} 1 & a & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 \\ 0 & b+2a & a+6 & 2 & 1 & 0 \end{array}\right]$$

Επειδή δεν χωρίζαμε αν $b+2a \neq 0$ δεν μπορώ να διαιρέσω με $b+2a$ τη 2η γραμμή.

$$\xrightarrow[R_3 \to R_3 - (b+2a)R_2]{R_1 \to R_1 - aR_2} \left[\begin{array}{ccc|ccc} 1 & 0 & 3-2a & 1 & 0 & -a \\ 0 & 1 & 2 & 0 & 0 & 1 \\ 0 & 0 & -2b-3a+6 & 2 & 1 & -b-2a \end{array}\right]$$

Εδώ πρέπει να διακρίνουμε υποχρεωτικά περιπτώσεις.

- Αν $-2b-3a+6=0$, τότε έχουμε μια μηδενική γραμμή, δηλαδή η μήτρα A δεν αντιστρέφεται. Αυτή την περίπτωση. $3a+2b=6$

• Αν $-2b-3a+6 \neq 0$, τότε μπορούμε να διαιρέσουμε την 3η γραμμή με αυτό και να συνεχίσουμε την διαδικασία.

$R_3 \to \frac{1}{-2b-3a+6} R_3$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 3-2a & 1 & 0 & a \\ 0 & 1 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & \frac{2}{6-3a-2b} & \frac{1}{6-3a-2b} & \frac{-b-2a}{6-2b-3a} \end{array}\right]$$

$R_1 \to R_1-(3-2a)R_3$

$R_2 \to R_2-2R_3$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1-\frac{2(3-2a)}{6-3a-2b} & -\frac{3-2a}{6-3a-2b} & a-\frac{(3-2a)(-b-2a)}{6-3a-2b} \\ 0 & 1 & 0 & \frac{-4}{6-3a-2b} & \frac{-2}{6-3a-2b} & 1-\frac{2(-b-2a)}{6-3a-2b} \\ 0 & 0 & 1 & \frac{2}{6-3a-2b} & \frac{1}{6-3a-2b} & \frac{-b-2a}{6-2b-3a} \end{array}\right]$$

Άρα, αν $-2b-3a+6 \neq 0$ τότε

$$A^{-1} = \begin{bmatrix} 1-\frac{2(3-2a)}{6-3a-2b} & -\frac{3-2a}{6-3a-2b} & a-\frac{(3-2a)(-b-2a)}{6-3a-2b} \\ \frac{-4}{6-3a-2b} & \frac{-2}{6-3a-2b} & 1-\frac{2(-b-2a)}{6-3a-2b} \\ \frac{2}{6-3a-2b} & \frac{1}{6-3a-2b} & \frac{-b-2a}{6-3a-2b} \end{bmatrix}$$

Πρόβλημα

Δίνονται 3 πίνακες $n \times n$ A, B, C.
Να εξεταστεί αν $AB = C$.

Θα δοθεί ένας "πιθανοτικός" αλγόριθμος που απαντά στο ερώτημα όταν τα στοιχεία των A, B, C είναι φυσικοί αριθμοί.

Ο κλασικός τρόπος είναι να υπολογίσουμε το γινόμενο AB και να ελέγξουμε αν ισούται με το C.
Στην περίπτωση αυτή χρειαζόμαστε
n^3 πολλαπλασιασμούς και $n^2(n-1)$ προσθέσεις

No. Date

Έστω n η μέγιστη τιμή των στοιχείων των μητρών A, B, C τότε προκύπτει ότι η μέγιστη δυνατή τιμή των στοιχείων της μήτρας AB ισούται με $n \cdot m^2$.
Θεωρούμε ότι τα στοιχεία των μητρών A, B, C ανήκουν στο σώμα $\mathbb{F}_p$ όπου p πρώτος μεγαλύτερος από το $n \cdot m^2$.
Επίσης θεωρούμε ότι οι πράξεις και οι πολλαπλοί μεταξύ των στοιχείων των μητρών γίνονται στο σώμα $\mathbb{F}_p$ (η πρόσθεση και ο πολλαπλασιασμός modulo p).

Επιλέγουμε τυχαίο μια μήτρα στήλη $n \times 1$ $r = \begin{bmatrix} a_1 \\ a_2 \\ a_n \end{bmatrix}$ όπου τα a_i επιλέγονται τυχαία και ανεξάρτητα από το σύνολο $\{0, 1, 2, \dots, p-1\}$

Θα πολλαπλασιάσουμε το r με τα A B και C ως εξής
$(AB)r = Cr$
Πρώτα το (Br) και έπειτα το $A(Br)$ και τέλος το Cr.

Για το Br ($n \times n$, $n \times 1$) χρειάζονται n^2 πολλαπλασιασμοί

Για το $A(Br)$ ($n \times n$, $n \times 1$) χρειάζονται n^2 πολλαπλασιασμοί.

Για το Cr χρειάζονται n^2 πολλαπλασιασμοί.

Άρα, συνολικά $3n^2$ πολλαπλασιασμοί.

Θα δείξουμε ότι $AB \neq C$ τότε $ABr \neq Cr$ με πιθανότητα μεγαλύτερη ή ίση από το $1/2$.

Απόδειξη

Έστω $D = AB - C$, τότε $D \neq 0_n$.

Άρα, υπάρχει μια τουλάχιστον μήτρα $n \times 1$ g ώστε $Dg \neq 0_n$.

Θα δείξαμε ότι για κάθε r που μηδενίζει την D υπάρχει ένα r' για το οποίο $Dr' \neq 0$.

Ορίσαμε για κάθε r που μηδενίζει το μηδενικό Dr ως $r' = g + r$. Τότε το $Dr' = D(g+r) = Dg + Dr = Dg \neq 0_n$.

Άρα τα r' που δεν μηδενίζουν το D είναι περισσότερα από αυτά που το μηδενίζουν.

Επίσης, αυτό ισχύει γιατί αν το $r_1' = r_2' \iff r_1 + g = r_2 + g \iff$
$\iff r_1 = r_2$.
Δηλαδή, για κάθε r_1, r_2 που μηδενίζει το D υπάρχει διαφορετικό r_1', r_2' που δεν το μηδενίζει.

Άσκηση 3 (Άσκηση από Εξετάσεις)

Να δειχθεί ότι κάθε μήτρα A $n \times n$ γράφεται κατά μοναδικό τρόπο ως άθροισμα μιας συμμετρικής μήτρας και μιας στρεβλά συμμετρικής μήτρας.

Υπενθύμιση:
D συμμετρική $\iff D = D^t$
D στρεβλά συμμετρική $\iff D = -D^t$

Έστω ότι υπάρχει B συμμετρική και C στρεβλά συμμετρική, ώστε

$$A = B + C \quad (1)$$

Τότε

$$A^t = (B+C)^t = B^t + C^t = B - C \quad (2)$$

① + ② $\quad 2B = A + A^t \Leftrightarrow B = \frac{1}{2}(A + A^t)$

① − ② $\quad 2C = A - A^t \Leftrightarrow C = \frac{1}{2}(A - A^t)$

Δείξαμε ότι αν υπάρχουν B, C τότε είναι μοναδικές.
Θα δείξουμε ότι B συμμετρική, C αντισυμμετρική.

$$B^t = \left(\tfrac{1}{2}(A + A^t)\right)^t = \tfrac{1}{2}(A + A^t)^t =$$

$$= \tfrac{1}{2}(A^t + (A^t)^t) = \tfrac{1}{2}(A^t + A) = B$$

Άρα, B συμμετρική

$$C^t = \left(\tfrac{1}{2}(A - A^t)\right)^t = \tfrac{1}{2}(A - A^t)^t = \tfrac{1}{2}(A^t - A) = -C$$

Άρα η C είναι αντισυμμετρική.

Άσκηση 4 (Εφαρμογή)

Να βρεθούν όλες οι μήτρες B που αντιμετατίθενται με την μήτρα

$$A_1 = \begin{bmatrix} a & 0 \\ a & a \end{bmatrix} \quad a \in \mathbb{R}^*.$$

Έστω $B = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$

Θεωρούμε την εξίσωση

$$A_1 B = B A_1$$

$$\begin{bmatrix} a & 0 \\ a & a \end{bmatrix}\begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}\begin{bmatrix} a & 0 \\ a & a \end{bmatrix} \Leftrightarrow$$

$$\begin{bmatrix} ax & ay \\ a(x+z) & a(y+w) \end{bmatrix} = \begin{bmatrix} a(x+y) & ay \\ a(z+w) & aw \end{bmatrix} \Leftrightarrow$$

$$\begin{cases} ay=ay \\ ax=ax+ay \\ a(x+z)=a(z+w) \\ ay+aw=aw \end{cases} \Leftrightarrow \begin{cases} ay=0 \\ ax+az=az+aw \end{cases} \Leftrightarrow \begin{cases} y=0 \\ w=x \end{cases}$$

Άρα $x\in\mathbb{R}$, $y=0$, $z\in\mathbb{R}$, $w=x$

Οπότε οι ζητούμενες μήτρες έχουν την μορφή

$$B=\begin{bmatrix} x & 0 \\ z & x \end{bmatrix}, \text{ όπου } x,z\in\mathbb{R}$$

Άσκηση 5 (Εργασία Άσκηση 13)

Έστω $\sigma: X\to X$ με $\sigma(\sigma(x))=x$ για κάθε $x\in X$. Να δειχθεί ότι η σ είναι μετάθεση του X.

Θα δείξουμε ότι σ είναι 1-1 και επί.
Έστω $\sigma(x_1)=\sigma(x_2) \Leftrightarrow \sigma(\sigma(x_1))=\sigma(\sigma(x_2)) \Leftrightarrow x_1=x_2$
Άρα, η σ είναι 1-1.

Θα δείξουμε ότι η σ είναι επί.
Έστω $y\in X$. Θα δείξουμε ότι υπάρχει $z\in X$ ώστε $\sigma(z)=y$.
Θέτουμε $z=\sigma(y)$, τότε $\sigma(z)=\sigma(\sigma(y))=y$
Άρα, η σ είναι επί.
Άρα, η σ είναι μετάθεση.

Άσκηση 6

α) Έστω ότι $A, B\in M_n$ αντιστρέψιμες.
Να δειχθεί ότι

$$B^{-1}=A^{-1}-B^{-1}(B-A)A^{-1}$$

Αρκεί να δείξουμε ότι $B(A^{-1}-B^{-1}(B-A)A^{-1})=I_n$

Πράγματι

$$B(A^{-1} - B^{-1}(B-A)A^{-1}) = BA^{-1} - B\,B^{-1}(B-A)A^{-1} =$$
$$= BA^{-1} - (B-A)A^{-1} = BA^{-1} - BA^{-1} + AA^{-1} =$$
$$= A\,A^{-1} = I_n$$

β) Έστω A αντιστρέψιμη και $A+B$ αντιστρέψιμη. Να δειχθεί ότι

$$(A+B)^{-1} = A^{-1} - A^{-1}BA^{-1} + (A+B)^{-1}(BA^{-1})^2$$

Στην προηγούμενη σχέση θέτουμε $B = A+B$

$$(A+B)^{-1} = A^{-1} - (A+B)^{-1}BA^{-1} = A^{-1} - (A^{-1} - (A+B)^{-1}BA^{-1})BA^{-1} =$$
$$= A^{-1} - A^{-1}BA^{-1} + (A+B)^{-1}BA^{-1}BA^{-1} = A^{-1} - A^{-1}BA^{-1} + (A+B)^{-1}(BA^{-1})^2$$

γ) Ο τύπος Sherman - Morrison - Woodbury

Αν A είναι αντιστρέψιμη U, V είναι $n \times k$ τότε

$$(A+UV^t)^{-1} = A^{-1} - A^{-1}U(I + V^tA^{-1}U)^{-1}V^tA^{-1}$$

Ειδικά, για $k=1$ έχουμε ότι

$$(A+UV^t)^{-1} = A^{-1} - \frac{1}{a}A^{-1}UV^tA^{-1}$$

όπου a είναι το στοιχείο της 1×1 μήτρας $I + V^tAU$.

Άσκηση 7 (Εργασία Άσκηση 5)

Να προσδιορισθούν όλες οι αδύναμες μήτρες

$$A = \begin{bmatrix} a & b \\ 1 & c \end{bmatrix}$$

Πρέπει $A^2 = A$

$$\begin{bmatrix} a & b \\ 1 & c \end{bmatrix}\begin{bmatrix} a & b \\ 1 & c \end{bmatrix} = \begin{bmatrix} a & b \\ 1 & c \end{bmatrix}$$

$$\begin{bmatrix} a^2+b & ab+bc \\ a+c & b+c^2 \end{bmatrix} = \begin{bmatrix} a & b \\ 1 & c \end{bmatrix}$$

$$\begin{aligned} &a^2+b=a \\ &b(a+c)=b \\ &a+c=1 \\ &b+c^2=c \end{aligned} \iff \begin{cases} a^2+b=a \\ a+c=1 \\ b+c^2=c \end{cases} \iff \begin{cases} c=1-a \\ b+(1-a)^2=1-a \\ a^2+b=a \end{cases} \iff$$

$$\iff \begin{cases} c=1-a \\ b+1+a^2-2a=1-a \\ a^2+b=a \end{cases} \iff \begin{cases} c=1-a \\ b+a^2=a \\ a^2+b=a \end{cases} \iff \begin{cases} c=1-a \\ \\ b+a^2=a \end{cases}$$

$$\iff \begin{cases} c=1-a \\ b=a-a^2 \end{cases}$$

Άρα, πρέπει

$$A=\begin{bmatrix} a & a-a^2 \\ 1 & 1-a \end{bmatrix}, a\in\mathbb{R}$$

Το Τεστ του Fermat

Δίνεται ένας φυσικός αριθμός n.
Ζητείται να εξεταστεί αν ο n είναι πρώτος ή όχι.

Επιλέγουμε τυχαία $a\in\{1,2,\dots,n-1\}$
Αν $a^n\equiv a \bmod n$
τότε επανέλαβε για άλλο a.

Αν $a^n\not\equiv a \bmod n$
για κάποιο a τότε ο n είναι σύνθετος

Αν $a^n\equiv a \bmod n$ για α διαφορετικά a

Τότε η πιθανότητα ο n να είναι σύνθετος είναι $\leq \frac{1}{2^k}$.

σύνθετος: έχει και άλλους ακέραιους διαιρέτες εκτός του 1, η.

Π.χ. $n=33$

Διαλέγουμε τυχαία $a \in \{1,2,\dots,32\}$ π.χ. $a=17$.

Υπολογίζουμε το

$$17^{33} \bmod 33$$

Αν το αποτέλεσμα <u>δεν είναι 17</u>, τότε το 33 είναι σύνθετος.

Αν το αποτέλεσμα είναι 17, δοκιμάζουμε ξανά.

Θεώρημα Euler-Fermat

Αν $a, n \in \mathbb{N}^*$ και $\text{μκδ}(a,n)=1$ τότε

$$a^{\phi(n)} \equiv 1 \bmod n$$

Αν n είναι πρώτος, τότε $\phi(n)=n-1$

$a^{n-1} \equiv 1 \bmod n$, για κάθε a με $\text{μκδ}(a,n)=1$

$a^{n-1} \equiv 1 \bmod n$, για κάθε $a \in \{1,2,\dots,n-1\}$

Άρα, συνοψίζοντας

$a^n \equiv a \bmod n$, αν n πρώτος για κάθε $a \in \{1,2,3,\dots,n-1\}$

Πρόταση

Το υποσύνολο U_n των $a \in \{1,2,\dots,n-1\}$ ώστε $\text{μκδ}(a,n)=1$ εφοδιασμένο με την πράξη του πολλαπλασιασμού modulo n είναι ομάδα, για κάθε $n \in \mathbb{N}^*$.

Αν $H \subseteq G$ όπου G ομάδα και το H είναι κλειστό ως προς την πράξη της ομάδας, τότε το H λέγεται **υποομάδα** της G.

Τότε, το πλήθος των στοιχείων του H διαιρεί το πλήθος των στοιχείων του G, δηλαδή $|H||G|$

Πόρισμα

Αν H υποομάδα της G και $H \neq G$, τότε
$$|H| \leq \frac{|G|}{2}$$

Πρόταση

Το σύνολο των $a \in \{1, 2, \dots, n-1\}$ με $\text{μκδ}(a, n) = 1$ και $a^n \equiv a \bmod n$ είναι υποομάδα της U_n.

Συμπέρασμα

Αν υπάρχει έστω ένα $a \in \{1, 2, \dots, n-1\}$ ώστε $a^n \neq a \bmod n$, τότε υπάρχουν τουλάχιστον $\frac{n}{2}$ στοιχεία a με $a^n \neq a \bmod n$ (αφού η υποομάδα με $a^n \equiv a \bmod n$ θα έχει το πολύ $n/2$ στοιχεία).
Άρα, η πιθανότητα να είναι $a^n \equiv a \bmod n$ είναι $\leq \frac{1}{2}$ για κάποιο a.

No. Date