UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
APPLIED ALGEBRA - MEM244 (FALL SEMESTER 2018-19)
LECTURER: G. KAPETANAKIS

FINAL EXAM – JANUARY 2019

1. i. Let $\sqrt{-5}$ be a root of $X^2+5 \in \mathbb{Z}[X]$. Show that 3 is irreducible, but not prime in $\mathbb{Z}[\sqrt{-5}]$.
   ii. Find all the primitive elements of $\mathbb{F}_{25}$.
   iii. Compute $\phi(31)$ and find (or describe) all the primitive elements of $\mathbb{F}_{32}$.

2. i. Show that $f(X) = X^3 - X - 2 \in \mathbb{F}_5[X]$ is irreducible.
   ii. Let $\alpha \in \mathbb{F}_{5^3}$ be a root of f. Express all the roots of f with respect to the basis $\{1, \alpha, \alpha^2\}$.
   iii. Compute $\mathrm{Tr}(\alpha)$.
   iv. Find some $\beta \in \mathbb{F}_{5^3}$ such that $\mathrm{Tr}(\beta) = 1$.

3. i. Find the least prime p such that $X^{18} + X^{17} + \cdots + X + 1$ is irreducible over $\mathbb{F}_p$.
   ii. Factor $X^8 - 1$ over $\mathbb{F}_3$.

4. Let C be the binary linear code with parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

   i. Write a generator matrix of C and find the parameters of C. How many errors does C correct?
   ii. List all the codewords of C and decode the words $w_1 = 110110$ and $w_2 = 011011$.

5. Let C be a code over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{pmatrix}.$$

   i. Show that C is an MDS code.
   ii. Write a generator matrix of the dual code $C^\perp$.
   iii. Show that $C^\perp$ is an MDS code.

---

1. All exercises are equivalent, with a maximum of 10 points.
2. The duration of the exam is 2.5 hours and you are allowed to leave the classroom the earliest 30 minutes after the beginning of the exam.
3. During the exam you are not allowed to have any bags, notes, books or electronics (calculators, mobiles, tablets, laptops etc.) on or next to you.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΕΦΑΡΜΟΣΜΕΝΗ ΑΛΓΕΒΡΑ - ΜΕΜ244 (ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2018-19)
ΔΙΔΑΣΚΩΝ: Γ. ΚΑΠΕΤΑΝΑΚΗΣ

ΤΕΛΙΚΗ ΕΞΕΤΑΣΗ – ΙΑΝΟΥΑΡΙΟΣ 2019

1. i. Έστω $\sqrt{-5}$ ρίζα του $X^2+5 \in \mathbb{Z}[X]$. Δείξτε ότι το 3 είναι ανάγωγο, αλλά όχι πρώτο στον $\mathbb{Z}[\sqrt{-5}]$.
   ii. Βρείτε όλα τα πρωταρχικά στοιχεία του $\mathbb{F}_{25}$.
   iii. Υπολογίστε το $\phi(31)$ και βρείτε (ή περιγράψτε) όλα τα πρωταρχικά στοιχεία του $\mathbb{F}_{32}$.

2. i. Δείξτε ότι το $f(X) = X^3 - X - 2 \in \mathbb{F}_5[X]$ είναι ανάγωγο.
   ii. Έστω $\alpha \in \mathbb{F}_{5^3}$ ρίζα του f. Γράψτε όλες τις ρίζες του f ως προς την βάση $\{1, \alpha, \alpha^2\}$.
   iii. Υπολογίστε το $\mathrm{Tr}(\alpha)$.
   iv. Βρείτε κάποιο $\beta \in \mathbb{F}_{5^3}$ τέτοιο ώστε $\mathrm{Tr}(\beta) = 1$.

3. i. Βρείτε τον ελάχιστο πρώτο p τέτοιον ώστε το $X^{18} + X^{17} + \cdots + X + 1$ να είναι ανάγωγο υπέρ του $\mathbb{F}_p$.
   ii. Παραγοντοποιείστε το $X^8 - 1$ στο $\mathbb{F}_3$.

4. Έστω C ο δυαδικός γραμμικός κώδικας με πίνακα ελέγχου τον

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

   i. Γράψτε έναν γεννήτορα πίνακα του C και βρείτε τις παραμέτρους του C. Πόσα λάθη διορθώνει ο C;
   ii. Γράψτε όλες τις κωδικολέξεις του C και αποκωδικοποιείστε τις λέξεις $w_1 = 110110$ και $w_2 = 011011$.

5. Έστω C κώδικας υπέρ του $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ με γεννήτορα πίνακα

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{pmatrix}.$$

   i. Δείξτε ότι ο C είναι MDS.
   ii. Γράψτε έναν γεννήτορα πίνακα του δυϊκού κώδικα $C^\perp$.
   iii. Δείξτε ότι ο $C^\perp$ είναι MDS.

---

1. Όλα τα θέματα είναι ισοδύναμα και άριστα είναι το 10.
2. Η διάρκεια της εξέτασης είναι 2,5 ώρες και μπορείτε να αποχωρίσετε από την αίθουσα το νωρίτερο 30 λεπτά μετά την αρχή της εξέτασης.
3. Κατά την διάρκεια της εξέτασης δεν επιτρέπεται να έχετε πάνω σας ή δίπλα σας τσάντες, σημειώσεις, βιβλία ή ηλεκτρονικές συσκευές (αριθμομηχανές, κινητά, ταμπλέτες, φορητούς υπολογιστές κτλ.).