Τμήμα Μαθηματικών, Πανεπιστημίου Κρήτης
Εξεταστική περίοδος Ιουνίου ακαδημαϊκού έτους 2009-2010
Παρασκευή, 18 Ιουνίου 2010

Εφαρμοσμένη Άλγεβρα

Διδάσκων: Α. Τόγκας

Θέματα

(Δικαιολογείστε πλήρως όλες τις απαντήσεις σας)

Θέμα 1 (1 μονάδα)

α) Να κατασκευασθεί ο πίνακας του σώματος $\mathbb{F}_{3^2} = \mathbb{F}_3[x]/x^2+x+2$ και να βρεθούν τα ελάχιστα πολυώνυμα των στοιχείων του.

β) Αν $\alpha \in \mathbb{F}_{3^2}$ μια ρίζα του x^2+x+2, να βρεθεί μια ρίζα του x^2+1.

γ) Να βρεθούν τα αντίστροφα στοιχεία ως προς τον πολλαπλασιασμό των $\alpha+2$ και $2\,\alpha+2$.

Θέμα 2 (1 μονάδα)

α) Να βρεθούν όλα τα υποσώματα των πεπερασμένων σωμάτων (i) $\mathbb{F}_{2^{18}}$ και (ii) $\mathbb{F}_{3^{40}}$ και να κατασκευασθεί το πλέγμα υποσωμάτων τους.

β) Να βρεθεί το πλήθος των ανάγωγων και το πλήθος των πρωταρχικών πολυωνύμων βαθμού 8 πάνω στο $\mathbb{F}_2$. (Σημειώστε ότι $255 = 3 \cdot 5 \cdot 17$)

Θέμα 3 (2 μονάδες)

α) Χρησιμοποιώντας το κριτήριο που βασίζεται στον αλγόριθμο του Berlekamp να αποδειχθεί ότι το πολυώνυμο $f(x) = x^4+x+1$ είναι ανάγωγο στο $\mathbb{F}_2[x]$.

β) Χρησιμοποιώντας τον αλγόριθμο του Berlekamp να παραγοντοποιηθεί σε γινόμενα ανάγωγων πολυωνύμων το $f(x) = x^3+x+1$ στο $\mathbb{F}_3[x]$.

Θέμα 4 (1 μονάδα)

α) Χρησιμοποιώντας τα κυκλοτομικά πολυώνυμα να παραγοντοποιηθεί σε γινόμενο ανάγωγων πολυωνύμων το x^9-1 πάνω στο $\mathbb{F}_2$.

β) Να υπολογιστούν τα κυκλοτομικά πολυώνυμα (i) $Q_{18}(x)$ και (ii) $Q_{24}(x)$ πάνω στο σώμα $\mathbb{F}_2$.

Θέμα 5 (1 μονάδα)

Για καθένα από τα παρακάτω κυκλοτομικά πολυώνυμα να διερευνηθεί αν είναι ανάγωγο ή όχι πάνω στο δοσμένο σώμα. Για εκείνα που δεν είναι ανάγωγα να βρεθεί το πλήθος των ανάγωγων πολυωνύμων που αναλύονται.

(i) $Q_{10}(x)$ στο $\mathbb{F}_3$, (ii) $Q_{12}(x)$ στο $\mathbb{F}_5$, (iii) $Q_{13}(x)$ στο $\mathbb{F}_3$, (iv) $Q_{14}(x)$ στο $\mathbb{F}_{11}$.

Θέμα 6 (2 μονάδες) Θεωρούμε δυαδική κωδικο-συνάρτηση $f : B^3 \to B^6$ με γεννήτορα πίνακα

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

α) Να βρεθεί πόσα λάθη εντοπίζει και πόσα διορθώνει ο κώδικας.

β) Να βρεθεί ο πίνακας συνδρόμων-πλευρικών οδηγών της f.

γ) Ένα μήνυμα κωδικοποιείται με την εξής αντιστοιχία

000 _	100 A	010 B	001 D
011 E	101 R	110 K	111 N

και λαμβάνουμε 011101, 110000, 101110. Να αποκωδικοποιηθεί το μήνυμα.

Θέμα 7 (2 μονάδες)

α) Να βρεθεί το πολυώνυμο-γεννήτορας του ελάχιστου δυαδικού κυκλικού κώδικα μήκους 7 που περιέχει την κωδικολέξη 1001110.

β) Έστω C ο δυαδικός κυκλικός κώδικας μήκους 7 με πολυώνυμο γεννήτορα το $g(x) = 1+x+x^2+x^4$. Μια λέξη κωδικοποιείται με τον C και λαμβάνεται ως $w = 1010100$. Να αποκωδικοποιηθεί η λέξη w, δεδομένου ότι ο C εντοπίζει 2-λάθη και διορθώνει 1-λάθη.

Καλό καλοκαίρι

Ενδεικτικές απαντήσεις των θεμάτων

Θέμα 1

α) Μας ζητείται να κατασκευάσουμε τον πίνακα του σώματος $\mathbb{F}_{3^2}$ ως την επέκταση $\mathbb{F}_3[x]/x^2+x+2$ του ελάχιστου υποσώματος $\mathbb{F}_3$ και να βρεθούν τα ελάχιστα πολυώνυμα των στοιχείων του.

Έστω $\alpha \in \mathbb{F}_{3^2}$ μια ρίζα του $p(x) = x^2 + x + 2$. Μπορούμε να αναπαραστήσουμε τα στοιχεία του $\mathbb{F}_{3^2}$ στην μορφή $f(a)$ όπου $f(x)$ είναι τα $3^2 = 9$ πολυώνυμα στο $\mathbb{F}_3$ βαθμού $d \leq 1$. Αφού $p(a) = 0$ τότε

$$\alpha^2 + \alpha + 2 = 0 \Rightarrow \alpha^2 = -\alpha - 2 \Rightarrow \alpha^2 = 2\alpha + 1\,, \tag{1}$$

($-1 \equiv 2 \mod 3$ και $-2 \equiv 1 \mod 3$). Επιπλέον έχουμε

$$\begin{aligned}
\alpha^8 &= (\alpha^4)^2 \\
&= (\alpha^2\,\alpha^2)^2 \\
&= (2\alpha+1)^2\,(2\alpha+1)^2 \\
&= (4\alpha^2+4\alpha+1)\,(4\alpha^2+4\alpha+1) && (4 \equiv 1 \mod 3) \\
&= (\alpha^2+\alpha+1)\,(\alpha^2+\alpha+1) && (\alpha^2 = 2\alpha+1) \\
&= (2\alpha+1+\alpha+1)\,(2\alpha+1+\alpha+1) \\
&= (3\alpha+2)\,(3\alpha+2) && (3 \equiv 0 \mod 3\,, 4 \equiv 1 \mod 3) \\
&= 1
\end{aligned}$$

Αφού $\alpha^2 \neq 1$, $\alpha^4 \neq 1$ και $|\alpha| \mid 8$ τότε $\alpha^8 = 1$ και συνεπώς το α είναι πρωταρχική ρίζα, οπότε

$$\mathbb{F}_{3^2} = \{0, 1, \alpha, \alpha^2, \ldots \alpha^7\}\,.$$

Χρησιμοποιώντας το γεγονός ότι $\alpha^2 = 2\alpha + 1$, έχουμε ότι

$$\begin{aligned}
\alpha^3 &= \alpha\,\alpha^2 = \alpha(2\alpha+1) = 2\alpha^2+\alpha = 2(2\alpha+1)+\alpha = 5\alpha+2 = 2\alpha+2 && (\equiv \mod 3) \\
\alpha^4 &= \alpha\,\alpha^3 = \alpha(2\alpha+2) = 2\alpha^2+2\alpha = 2(2\alpha+1)+2\alpha = 6\alpha+2 = 2 && (\equiv \mod 3) \\
\alpha^5 &= \alpha\,\alpha^4 = 2\alpha \\
\alpha^6 &= \alpha\,\alpha^5 = 2\alpha^2 = 2(2\alpha+1) = 4\alpha+2 = \alpha+2 \\
\alpha^7 &= \alpha\,\alpha^6 = \alpha(\alpha+2) = \alpha^2+2\alpha = 2\alpha+1+2\alpha = 4\alpha+1 = \alpha+1
\end{aligned}$$

Συνεπώς ο πίνακας του σώματος δίνεται από τον παρακάτω πίνακα

k	a_1	a_0
0	0	1
1	1	0
2	2	1
3	2	2
4	0	2
5	2	0
6	1	2
7	1	1

όπου k δηλώνει τον εκθέτη του στοιχείου α^k και $a_1\,, a_0$, οι συντελεστές του πολυωνύμου $f(x) = a_1\,x + a_0$.

Για τα ελάχιστα πολυώνυμα γνωρίζουμε ότι αν α είναι ρίζα ενός ανάγωγου πολυωνύμου $m(x)$ βαθμού d τότε και τα d στοιχεία

$$\{a, \Phi(a)\,, \ldots \Phi^{d-1}(a)\}$$

είναι κι αυτά ρίζες του $m(x)$, όπου Φ ο αυτομορφισμός Frobenius $\Phi(\alpha) = \alpha^p$, στην συγκεκριμένη περίπτωση $p = 3$. Χρησιμοποιώντας το γεγονός ότι $\alpha^8 = 1$, διακρίνουμε τις εξής περιπτώσεις :

Συζυγή στοιχεία του α:	α, $\Phi(\alpha) = \alpha^3$, $\Phi^2(a) = \alpha^9 = \alpha\,\alpha^8 = \alpha$	άρα α, α^3
Συζυγή στοιχεία του α^2	α^2, $\Phi(\alpha^2) = \alpha^6$, $\Phi^2(\alpha^2) = \alpha^{18} = \alpha^9\,\alpha^9 = \alpha\,\alpha = a^2$	άρα α^2, α^6
Συζυγή στοιχεία του α^4	α^4, $\Phi(\alpha^4) = \alpha^{12} = \alpha^4\,\alpha^8 = \alpha^4$	άρα α^4
Συζυγή στοιχεία του α^5	α^5, $\Phi(\alpha^5) = \alpha^{15} = \alpha^7\,\alpha^8 = \alpha^7$	άρα $\alpha^5\,, \alpha^7$

Σημειώνοντας με $m_k(x)$ το ελάχιστο πολυώνυμο του στοιχείου α^k έχουμε

$$m_1(x) = m_3(x) = (x-\alpha)(x-\alpha^3) = x^2 - (\alpha+\alpha^3)x + \alpha^4 = x^2 - (\alpha+2\alpha+2)x + 2 = x^2 + x + 2$$

$$m_2(x) = m_6(x) = (x-\alpha^2)(x-\alpha^6) = x^2 - (\alpha^2+\alpha^6)x + \alpha^8 = x^2 - (2\alpha+1+\alpha+2)x + 1 = x^2 + 1$$

$$m_4(x) = (x-\alpha^4) = x - 2$$

$$m_5(x) = m_7(x) = (x-\alpha^5)(x-\alpha^7) = x^2 - (\alpha^5+\alpha^7)x + \alpha^{12} = x^2 - (2\alpha+\alpha+1)x + \alpha^8\,\alpha^4 = x^2 + 2\alpha + 2$$

Τα υπόλοιπα ελάχιστα πολυώνυμα είναι τα $\mu_0(x) = x$, $\mu_1(x) = x - 1$ που αντιστοιχούν στα στοιχεία 0 και 1.

β) Από την προηγούμενη ανάλυση αμέσως συμπεραίνουμε ότι αν α είναι μια ρίζα του $x^2 + x + 2$, τότε μια ρίζα του $x^2 + 1$ είναι το στοιχείο α^2 ή το συζυγές του α^6.

γ) Από τον πίνακα του σώματος έχουμε ότι το $\alpha + 2$ αντιστοιχεί στο στοιχείο α^6. Αλλά $1 = \alpha^8 = \alpha^6\,\alpha^2$ κι έτσι το στοιχείο α^2 είναι το αντίστροφο του $\alpha + 2$, το οποίο από τον πίνακα αντιστοιχεί στο $2\alpha + 1$.

Ομοίως, το $2\alpha + 2$ αντιστοιχεί στο στοιχείο α^3, κι επειδή $1 = \alpha^8 = \alpha^3\,\alpha^5$, το στοιχείο α^5 είναι το αντίστροφο του $2\alpha + 2$, το οποίο από τον πίνακα αντιστοιχεί στο 2α.

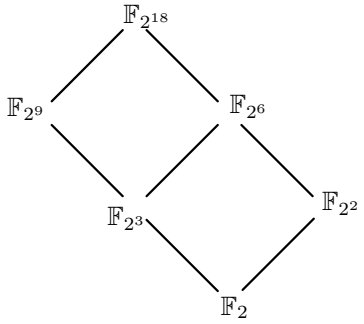
Θέμα 2

α) Από την θεωρία πεπερασμένων σωμάτων γνωρίζουμε ότι όλα τα δυνατά υποσώματα ενός πεπερασμένου σώματος $\mathbb{F}_{p^n}$, p πρώτος, n θετικός ακέραιος, είναι της μορφής $\mathbb{F}_{p^d}$ όπου $d \mid n$.

(i) Οι διαιρέτες του $n = 18$ είναι $1, 2, 3, 6, 9, 18$. Συνεπώς τα υποσώματα του $\mathbb{F}_{2^{18}}$ είναι τα :

$$\mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^3}, \mathbb{F}_{2^6}, \mathbb{F}_{2^9}, \mathbb{F}_{2^{18}}$$

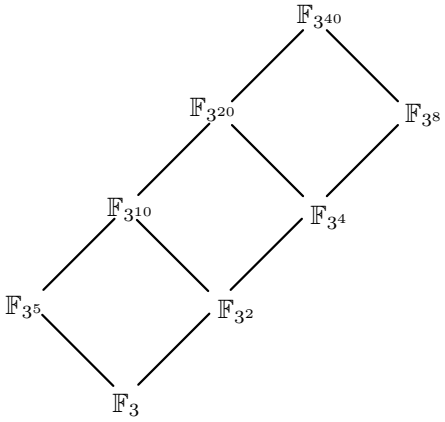
Το πλέγμα των υποσωμάτων δίνεται σχηματικά από το παρακάτω



(ii) Οι διαιρέτες του $n = 40$ είναι $1, 2, 4, 5, 8, 10, 20, 40$. Συνεπώς τα υποσώματα του $\mathbb{F}_{3^{40}}$ είναι τα :

$$\mathbb{F}_3, \mathbb{F}_{3^2}, \mathbb{F}_{3^4}, \mathbb{F}_{3^5}, \mathbb{F}_{3^8}, \mathbb{F}_{3^{10}}, \mathbb{F}_{3^{20}}, \mathbb{F}_{3^{40}}$$

Το πλέγμα των υποσωμάτων δίνεται σχηματικά από το παρακάτω



β) Από την θεωρία γνωρίζουμε ότι το πλήθος των ανάγωγων πολυωνύμων βαθμού n πάνω στο $\mathbb{F}_p$, δίνεται από τον τύπο

$$\Pi_p(n) = \frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})p^d$$

όπου

$$\mu(\frac{x}{y}) = \begin{cases} 1 & \text{αν} \quad x/y = 1 \\ (-1)^k & \text{αν} \quad x/y = p_1 p_2 \cdots p_k \quad \text{για διαφορετικούς πρώτους } p_i \\ 0 & \text{αλλιώς} \end{cases}$$

Οπότε

$$\begin{aligned} \Pi_2(8) &= \frac{1}{8}\sum_{d|8}\mu(\frac{8}{d})2^d = \frac{1}{8}(\mu(8)2^1 + \mu(4)2^2 + \mu(2)2^4 + \mu(1)2^8) = \frac{1}{8}(0\,2^1 + 0\,2^2 + (-1)2^4 + 2^8) \\ &= \frac{1}{2^3}(2^8 - 2^4) = 2^5 - 2 = 32 - 2 = 30 \end{aligned}$$

Το πλήθος των πρωταρχικών πολυωνύμων βαθμού n πάνω στο $\mathbb{F}_p$ δίνεται από τον τύπο

$$\frac{\varphi(p^n - 1)}{n}$$

όπου $\varphi(n)$ η συνάρτηση του Euler. Οπότε

$$\begin{aligned} \frac{\varphi(2^8-1)}{8} &= \frac{\varphi(256-1)}{8} = \frac{\varphi(255)}{8} = \frac{\varphi(3\cdot 5\cdot 17)}{8} = \frac{\varphi(3)\varphi(5)\varphi(17))}{8} = \frac{(3-1)(5-1)(17-1)}{8} \\ &= \frac{2\cdot 4\cdot 16}{8} = 16 \end{aligned}$$

Συνεπώς υπάρχουν 30 ανάγωγα πολυώνυμα βαθμού 8 πάνω στο $\mathbb{F}_2$, από τα οποία τα 16 είναι πρωταρχικά.

Θέμα 3

α) Μια βάση του διανυσματικού χώρου $\mathbb{F}_2[x]/f(x)$ όπου $f(x) = x^4 + x + 1$ είναι η $e = \{1, \alpha, \alpha^2, \alpha^3\}$, όπου $\alpha = [x]_f$. Έχουμε την γραμμική απεικόνιση (αυτομορφισμό Frobenius) $\Phi(a) = a^2$. Εφαρμόζουμε την απεικόνιση Φ στην βάση e και έχουμε

$$\begin{aligned} \Phi(1) &= 1 \\ \Phi(\alpha) &= \alpha^2 \\ \Phi(\alpha^2) &= \alpha^4 = \alpha + 1 \qquad\qquad (\alpha^4 = \alpha + 1) \\ \Phi(\alpha^3) &= \alpha^6 = \alpha^2\alpha^4 = \alpha^2(\alpha+1) = a^3 + \alpha^2 \end{aligned}$$

οπότε ο πίνακας της Φ στην βάση e είναι ο

$$[\Phi]_{\{e\}} = \begin{array}{c} \\ 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & \alpha & \alpha^2 & \alpha^3 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Σύμφωνα με το κριτήριο που βασίζεται στον αλγόριθμο του Frobenius, το $f(x)$ είναι ανάγωγο αν και μόνο αν $\ker(\Phi) = 0$ και $\ker(\Phi - I) = \mathbb{F}_2$.
Για να βρούμε τον υπόχωρο $\ker\,\Phi$: Για το παρακάτω ομογενές γραμμικό σύστημα έχουμε ότι

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \Leftrightarrow \quad \begin{aligned} x_1 + x_3 &= 0 \\ x_3 &= 0 \\ x_2 + x_4 &= 0 \\ x_4 &= 0 \end{aligned} \quad \Rightarrow \quad \begin{aligned} x_1 &= 0 \\ x_2 &= 0 \\ x_3 &= 0 \\ x_4 &= 0 \end{aligned}$$

δηλαδή η μοναδική λύση είναι η μηδενική. Άρα $\ker\Phi = 0$.

Για να βρούμε τον υπόχωρο $\ker(\Phi - I)$: Για το παρακάτω ομογενές γραμμικό σύστημα έχουμε ότι

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \Leftrightarrow \quad \begin{aligned} x_3 &= 0 \\ x_2 + x_3 &= 0 \\ x_2 + x_3 + x_4 &= 0 \\ 0 &= 0 \end{aligned} \quad \Rightarrow \quad \begin{aligned} &x_1 \in \mathbb{F}_2 \text{ αυθαίρετο} \\ &x_2 = 0 \\ &x_3 = 0 \\ &x_4 = 0 \end{aligned}$$

άρα $\ker(\Phi - I) = \mathbb{F}_2$ και συνεπώς το $f(x) = x^4 + x + 1$ είναι ανάγωγο πάνω στο $\mathbb{F}_2$.

β) Μια βάση του διανυσματικού χώρου $\mathbb{F}_3[x]/f(x)$ όπου $f(x) = x^3 + x + 1$ είναι η $e = \{1, \alpha, \alpha^2\}$, όπου $\alpha = [x]_f$. Έχουμε την γραμμική απεικόνιση (αυτομορφισμό Frobenius) $\Phi(a) = a^3$. Εφαρμόζουμε την απεικόνιση Φ στην βάση e και έχουμε

$$\begin{aligned} \Phi(1) &= 1 \\ \Phi(\alpha) &= \alpha^3 = 2\alpha + 2 \\ \Phi(\alpha^2) &= \alpha^6 = \alpha^3\alpha^3 = (2\alpha+2)(2\alpha+2) = 4\alpha^2 + 8\alpha + 4 = \alpha^2 + 2\alpha + 1 \qquad (\equiv \mod 3) \end{aligned}$$

οπότε ο πίνακας της Φ στην βάση e είναι ο

$$[\Phi]_{\{e\}} = \begin{array}{c} \\ 1 \\ \alpha \\ \alpha^2 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & \alpha & \alpha^2 \end{array} \\ \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \qquad [\Phi]_{\{e\}} - I = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Για να βρούμε τον υπόχωρο $\ker(\Phi - I)$: Για το παρακάτω ομογενές γραμμικό σύστημα έχουμε ότι

$$\begin{pmatrix} 0 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \Leftrightarrow \quad \begin{aligned} 2x_2 + x_3 &= 0 \\ x_2 + 2x_3 &= 0 \\ 0 &= 0 \end{aligned} \quad \Rightarrow \quad \begin{aligned} &x_1 \in \mathbb{F}_2 \text{ αυθαίρετο} \\ &x_2 = x_3 \in \mathbb{F}_2 \end{aligned}$$

οπότε το τυχαίο $v \in \ker(\Phi - I)$ γράφεται ως

$$v = \begin{pmatrix} x_1 \\ x_2 \\ x_2 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

και $\ker(\Phi - I) = \{(1,0,0), (0,1,1)\}$. Το διάνυσμα $(0,1,1)$ αντιστοιχεί στο πολυώνυμο $h(x) = x + x^2$. Από τον αλγόριθμο του Berlekamp γνωρίζουμε ότι τα πολυώνυμα μ.κ.δ$(f(x), h(x))$, μ.κ.δ$(f(x), h(x) - 1)$ και μ.κ.δ$(f(x), h(x) - 2)$ είναι ανάγωγοι παράγοντες του $f(x)$. Εκτελώντας τον Ευκλείδιο αλγόριθμο διαίρεσης για την εύρεση μ.κ.δ. πολυωνύμων βρίσκουμε ότι:

$$\begin{aligned} \text{μ.κ.δ}(f(x), h(x)) &= 1 \\ \text{μ.κ.δ}(f(x), h(x) - 1) &= x^2 + x + 2 \\ \text{μ.κ.δ}(f(x), h(x) - 2) &= x + 2 \end{aligned}$$

οπότε

$$x^3 + x + 1 = (x + 2)(x^2 + x + 2)$$

είναι η ανάλυση σε ανάγωγα πολυώνυμα του $f(x) = x^3 + x + 1$.

Αναλυτικά έχουμε: Για το μ.κ.δ$(f(x), h(x))$

$$\begin{aligned} x^3 + x + 1 &= (x + 2)(x^2 + x) + (2x + 1) \\ x + x^2 &= (2x + 1)(2x + 1) + 2 \\ 2x + 1 &= 2(x + 2) \end{aligned}$$

Οπότε μ.κ.δ$(f(x), h(x)) = 1$ (όπως έχουμε δει αν το υπόλοιπο είναι μη-μηδενικό στοιχείο του $\mathbb{F}_3$ τότε αυτό μπορεί να αναχθεί στο στοιχείο 1).

Για το μ.κ.δ$(f(x), h(x) - 1)$

$$x^3 + x + 1 = (x + 2)(x^2 + x - 1)$$

Οπότε μ.κ.δ$(f(x), h(x) - 1) = x^2 + x - 1 = x^2 + x + 2 \quad (\equiv \mod 3)$

Για το μ.κ.δ$(f(x), h(x)-2)$

$$\begin{aligned} x^3+x+1 &= (x+2)(x^2+x-2)+(x+2) \\ x^2+x-2 &= (x+2)(x+2) \end{aligned}$$

Οπότε μ.κ.δ$(f(x), h(x)-2) = x+2$

Θέμα 4

α) Από την θεωρία των κυκλοτομικών πολυωνύμων γνωρίζουμε ότι για τα $Q_n(x)$ πάνω σ' ένα σώμα F χαρακτηριστικής p με $p \nmid n$ έχουμε

$$x^n - 1 = \prod_{d|n} Q_d(x)$$

Εδώ έχουμε το σώμα $\mathbb{F}_2$ και $n = 9$ και $2 \nmid 9$. Οι διαιρέτες του 9 είναι $1, 3, 9$, οπότε έχουμε

$$x^9 - 1 = Q_1(x)\, Q_3(x)\, Q_9(x)$$

Από τη θεωρία γνωρίζουμε ότι

$$\begin{aligned} Q_1(x) &= x-1 = x+1 \qquad (\equiv \mod 2) \\ Q_3(x) &= x^2+x+1 \end{aligned}$$

Προφανώς τα πολυώνυμα $Q_1(x), Q_3(x)$ είναι ανάγωγα πάνω στο $\mathbb{F}_2$ ($Q_3(0) = Q_3(1) = 1$). Αρκεί να υπολογίσουμε το πολυώνυμο $Q_9(x)$ και να βρούμε αν είναι ανάγωγο ή όχι. Στην περίπτωση που δεν είναι ανάγωγο θα πρέπει με κάποιον τρόπο να το παραγοντοποιήσουμε σε ανάγωγα πολυώνυμα.

Από τον ορισμό των κυκλοτομικών πολυωνύμων έχουμε ότι

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}$$

Οπότε

$$Q_9(x) = (x^9-1)^{\mu(1)}\,(x^3-1)^{\mu(3)}(x-1)^{\mu(9)}$$

Όμως $\mu(9) = \mu(3^2) = 0$, $\mu(3) = -1$ και $\mu(1) = 1$, οπότε

$$Q_9(x) = \frac{x^9-1}{x^3-1} = \frac{(x^3-1)(x^6+x^3+1)}{x^3-1} = x^6+x^3+1$$

Από το κριτήριο αναγωγιμότητας των κυκλοτομικών πολυωνύμων ξέρουμε ότι το $Q_n(x)$ είναι ανάγωγο πάνω στο $\mathbb{F}_p$, $p \nmid n$ αν και μόνο αν $o_n(p) = \varphi(n)$. Εδώ έχουμε για τον βαθμό του $Q_9(x)$ ότι

$$\varphi(9) = \varphi(3^2) = 3(3-1) = 6$$

Επιπλέον

$$\begin{aligned} 2 &\equiv 2 \mod 9 \\ 2^2 &\equiv 4 \mod 9 \\ 2^3 &\equiv 8 \mod 9 \\ 2^4 &\equiv 7 \mod 9 \\ 2^5 &\equiv 5 \mod 9 \\ 2^6 &\equiv 1 \mod 9 \end{aligned}$$

άρα $o_9(2) = 6 = \varphi(9)$ και συνεπώς το κυκλοτομικό πολυώνυμο $Q_9(x)$ είναι ανάγωγο πάνω στο $\mathbb{F}_2$. Τελικά έχουμε ότι η ανάλυση του $x^9 - 1$ σε ανάγωγα πολυώνυμα πάνω στο $\mathbb{F}_2$ είναι

$$x^9 - 1 = (x+1)(x^2+x+1)(x^6+x^3+1).$$

β) Για το υπολογισμό των κυκλοτομικών πολυωνύμων $Q_{18}(x)$ και $Q_{24}(x)$, έχουμε:

• $Q_{18}(x) = Q_{2\cdot 3^2}(x) = Q_{2\cdot 3}(x^3) = Q_6(x^3)$. Αρκεί να υπολογίσουμε το $Q_6(x)$. Από τον ορισμό των $Q_n(x)$ έχουμε

$$\begin{aligned} Q_6(x) &= (x^6-1)^{\mu(1)}\,(x^2-1)^{\mu(3)}(x^3-1)^{\mu(2)}(x-1)^{\mu(6)} = \frac{(x^6-1)(x-1)}{(x^2-1)(x^3-1)} = \frac{(x^3-1)(x^3+1)(x-1)}{(x-1)(x+1)(x^3-1)} \\ &= \frac{x^3+1}{x+1} = x^2-x+1 = x^2+x+1 \qquad (\equiv \mod 2) \end{aligned}$$

Συνεπώς πάνω στο $\mathbb{F}_2$ έχουμε

$$Q_{18}(x) = Q_6(x^3) = x^6+x^3+1$$

Ένας άλλος τρόπος υπολογισμού του $Q_{18}(x)$ βασίζεται στο γεγονός ότι πάνω σε ένα σώμα χαρακτηριστικής p ισχύει

$$Q_{np^k}(x) = Q_n(x)^{p^k-p^{k-1}}$$

Στο συγκεκριμένο θέμα θέλουμε να υπολογίσουμε το $Q_{18}(x)$ πάνω στο σώμα $\mathbb{F}_2$ το οποίο έχει χαρακτηριστική 2. Οπότε έχουμε

$$Q_{18}(x) = Q_{9\cdot 2}(x) = Q_9(x)^{2-1} = Q_9(x) = x^6+x^3+1$$

όπως βρήκαμε στο α) μέρος του θέματος.

• Για τον υπολογισμό του πολυωνύμου $Q_{24}(x)$ πάνω στο $\mathbb{F}_2$ χρησιμοποιούμε και πάλι την παραπάνω ιδιότητα και έχουμε
$Q_{24}(x) = Q_{3\cdot 2^3}(x) = Q_3(x)^{2^3-2^2} = Q_3(x)^4 = (x^2+x+1)^4 = (x^4+x^2+1)^2 = x^8+x^4+1$ πάνω στο $\mathbb{F}_2$.

Θέμα 5

Από το κριτήριο αναγωγιμότητας των κυκλοτομικών πολυωνύμων γνωρίζουμε ότι το $Q_n(x)$ είναι ανάγωγο πάνω στο $\mathbb{F}_p$, $p \nmid n$ αν και μόνο αν $o_n(p) = \varphi(n)$. Επιπλέον αν $d = o_n(p) \neq n$ τότε το $Q_n(x)$ αναλύεται σε $\varphi(n)/d$ διαφορετικά ανάγωγα πολυώνυμα πάνω στο $\mathbb{F}_p$, ίδιου βαθμού d.

(i) Για το $Q_{10}(x)$ στο $\mathbb{F}_3$ έχουμε:

$$\varphi(10) = \varphi(2\cdot 5) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4$$

Επιπλέον

$$\begin{aligned} 3 &\equiv 3 \mod 10 \\ 3^2 &\equiv 9 \mod 10 \\ 3^3 &\equiv 7 \mod 10 \\ 3^4 &\equiv 1 \mod 10 \end{aligned}$$

Άρα $o_{10}(3) = \varphi(10) = 4$ και συνεπώς το $Q_{10}(x)$ είναι ανάγωγο πάνω στο $\mathbb{F}_3$.

(ii) Για το $Q_{12}(x)$ πάνω στο $\mathbb{F}_5$ έχουμε:

$$\varphi(12) = \varphi(2^2\cdot 3) = \varphi(2^2)\varphi(3) = 2(2-1)(3-1) = 4$$

Επιπλέον

$$\begin{aligned} 5 &\equiv 5 \mod 12 \\ 5^2 &\equiv 1 \mod 12 \end{aligned}$$

Άρα $\varphi(12) = 4 \neq 2 = o_{12}(5)$ και συνεπώς το $Q_{12}(x)$ δεν είναι ανάγωγο πάνω στο $\mathbb{F}_5$. Το $Q_{12}(x)$ αναλύεται σε 2 ανάγωγα πολυώνυμα βαθμού 2.

(iii) Για το $Q_{13}(x)$ πάνω στο $\mathbb{F}_3$ έχουμε:

$$\varphi(13) = 13-1 = 12$$

Επιπλέον

$$\begin{aligned} 3 &\equiv 3 \mod 13 \\ 3^2 &\equiv 9 \mod 13 \\ 3^3 &\equiv 1 \mod 13 \end{aligned}$$

Άρα $\varphi(13) = 12 \neq 3 = o_{13}(3)$ και συνεπώς το $Q_{13}(x)$ δεν είναι ανάγωγο πάνω στο $\mathbb{F}_3$. Το $Q_{13}(x)$ αναλύεται σε 4 ανάγωγα πολυώνυμα βαθμού 3.

(iv) Για το $Q_{14}(x)$ πάνω στο $\mathbb{F}_{11}$ έχουμε:

$$\varphi(14) = \varphi(2 \cdot 7) = (2-1)(7-1) = 6$$

Επιπλέον

$$\begin{aligned} 11 &\equiv 11 \mod 14 \\ 11^2 &\equiv 9 \mod 14 \\ 11^3 &\equiv 1 \mod 14 \end{aligned}$$

Άρα $\varphi(14) = 6 \neq 3 = o_{14}(11)$ και συνεπώς το $Q_{14}(x)$ δεν είναι ανάγωγο πάνω στο $\mathbb{F}_{11}$. Το $Q_{14}(x)$ αναλύεται σε 2 ανάγωγα πολυώνυμα βαθμού 3.

Θέμα 6

α) Θεωρούμε την δυαδική κωδικο-συνάρτηση $f : B^3 \to B^6$ με γεννήτορα πίνακα

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Θα βρούμε πρώτα τις κωδικολέξεις της f πολλαπλασιάζοντας τα στοιχεία του B^3 με τον πίνακα G από αριστερά:

$$\begin{array}{cc} 000 & 000000 \\ 001 & 001101 \\ 010 & 010011 \\ 100 \xrightarrow{f} & 100110 \\ 011 & 011110 \\ 101 & 101011 \\ 110 & 110101 \\ 111 & 111000 \end{array}$$

Επειδή $\min \mathrm{d} = 3$, ο κώδικας εντοπίζει $3 - 1 = 2$-λάθη και διορθώνει $\left[\frac{3-1}{2}\right] = 1$ -λάθη.

β) Ο πίνακας ελέγχου-ισοτιμίας H του κώδικα με γεννήτορα-πίνακα G είναι ο

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

Με την βοήθεια του πίνακα H κατασκευάζουμε τον παρακάτω πίνακα συνδρόμων-πλευρικών οδηγών της f.

σύνδρομα	πλευρικοί οδηγοί
000	000000
001	000001
010	000010
100	000100
101	001000
011	010000
110	100000
111	010100

Ο παραπάνω πίνακας παράγεται παίρνοντας τους πλευρικούς οδηγούς (λέξεις μήκους 6 ελάχιστου βάρους) και πολλαπλασιάζοντας με τον πίνακα H από αριστερά. Αφού εξαντλήσουμε την περίπτωση πλευρικών οδηγών με ελάχιστο βάρος 1 (το ψηφίο 1 εμφανίζεται το πολύ μια φορά στην λέξη) παρατηρούμε ότι στην στήλη των αντίστοιχων σύνδρομων στοιχείων δεν έχουμε όλο το σύνολο B^3, γιατί το στοιχείο 111 απουσιάζει. Το 111 παράγεται, για

παράδειγμα ως $111 = 011 + 100$, με τα ήδη υπάρχοντα σύνδρομα στοιχεία και προσθέτοντας τους αντίστοιχους πλευρικούς οδηγούς έχουμε $010100 = 010000 + 000100$. Οπότε έχουμε ένα πλήρη πίνακα σύνδρομων-πλευρικών οδηγών.

γ) Το μήνυμα που λαμβάνουμε είναι 011101, 110000, 101110. Παρατηρούμε ότι καμιά λέξη που λάβαμε δεν είναι κωδικολέξη. Οπότε θα εφαρμόσουμε τον αλγόριθμο αποκωδικοποίησης για γραμμικούς κώδικες χρησιμοποιώντας τον πίνακα σύνδρομων-πλευρικών οδηγών που κατασκευάσαμε στο προηγούμενο β) μέρος. Για κάθε μια από τις λέξεις που λάβαμε βρίσκουμε το σύνδρομο της και προσθέτουμε στην λέξη τον αντίστοιχο πλευρικό οδηγό. Θέτουμε $w_1 = (0,1,1,1,0,1)$, $w_2 = (1,1,0,0,0,0)$, $w_3 = (1,0,1,1,1,0)$ και έχουμε

σύνδρομο		πλευρικός οδηγός	διορθωμένη λέξη	κωδικολέξη	αποκωδ/μένο μήνυμα
$w_1H = (0,1,1)$	$\rightarrow$	$e_1 = (0,1,0,0,0,0)$	$w_1 + e_1 = (0,0,1,1,0,1)$	001101	001 D
$w_2H = (1,0,1)$	$\rightarrow$	$e_2 = (0,0,1,0,0,0)$	$w_2 + e_2 = (1,1,1,0,0,0)$	111000	111 N
$w_3H = (1,0,1)$	$\rightarrow$	$e_3 = (0,0,1,0,0,0)$	$w_3 + e_3 = (1,0,0,1,1,0)$	100110	100 A

Θέμα 7

α) Μας ζητείται να βρούμε τον ελάχιστο κυκλικό κώδικα μήκους 7 που περιέχει την κωδικολέξη 1001110. Θέτουμε $f(x) = x^7 - 1$, και $h(x) = 1 + x^3 + x^4 + x^5$ το πολυώνυμο που αντιστοιχεί στην κωδικολέξη 1001110. Από την θεωρία των κυκλικών κωδίκων γνωρίζουμε ότι το πολυώνυμο-γεννήτορας που μας ζητείται είναι το

$$g(x) = \text{μ.κ.δ}(f(x), h(x))$$

Εκτελώντας τον Ευκλείδιο αλγόριθμο διαίρεσης για την εύρεση του μ.κ.δ πολυωνύμων βρίσκουμε ότι

$$x^7 - 1 = x^7 + 1 \quad (\equiv \mod 2) \quad = \quad (x + x^2)(1 + x^3 + x^4 + x^5) + (1 + x + x^2 + x^4)$$

$$(1 + x^3 + x^4 + x^5) \quad = \quad (x + 1)(1 + x + x^2 + x^4)$$

Συνεπώς $g(x) = 1 + x + x^2 + x^4$ είναι το ζητούμενο πολυώνυμο-γεννήτορας.

β) Έχουμε έναν κυκλικό κώδικα μήκους 7 με πολυώνυμο-γεννήτορα $g(x) = 1 + x + x^2 + x^4$, οπότε

$$C : B^3 \rightarrow B^7$$

Η λέξη που λήφθηκε είναι η $w = 1010100$ η οποία αντιστοιχεί στο πολυώνυμο $w(x) = 1 + x^2 + x^4$. Παρατηρούμε ότι

$$1 + x^2 + x^4 = (1 + x + x^2 + x^4) + x$$

οπότε $g(x) \nmid w(x)$ και συνεπώς η w δεν είναι κωδικολέξη και θα πρέπει να διορθωθεί με την υπόθεση ότι ο κώδικας C εντοπίζει 2-λάθη και διορθώνει 1-λάθη. Ο προηγούμενος υπολογισμός δείχνει ότι το σύνδρομο πολυώνυμο του $w(x)$ είναι

$$s(x) = w(x) \mod g(x) = x$$

Παρατηρούμε ότι το βάρος του πολυωνύμου $s(x)$ είναι $wt(s(x)) = 1 \leqslant 1$, οπότε δεν είναι αναγκαίο να συνεχίσουμε τον αλγόριθμο αποκωδικοποίησης για κυκλικούς κώδικες, και θέτουμε

$$e(x) = x^{7-0}s(x) \mod (x^7 + 1) = x^8 \mod (x^7 + 1) = x$$

Συνεπώς η διορθωμένη λέξη (πολυώνυμο) $\widetilde{w}(x)$ είναι

$$\widetilde{w}(x) = w(x) + e(x) = 1 + x + x^2 + x^4 = g(x)$$

Τελικά η λέξη (πολυώνυμο) που κωδικοποιήθηκε με τον κυκλικό κώδικα C είναι η

$$g(x)/g(x) = 1$$

που αντιστοιχεί στη λέξη $100 \in B^3$.