Τμήμα Μαθηματικών, Πανεπιστημίου Κρήτης
Εξεταστική περίοδος Σεπτεμβρίου ακαδημαϊκού έτους 2009-2010
Τρίτη, 31 Αυγούστου 2010

Εφαρμοσμένη Άλγεβρα

Διδάσκων: Α. Τόγκας

Θέματα

(Δικαιολογείστε πλήρως όλες τις απαντήσεις σας)

Θέμα 1 (1 μονάδα) Θεωρούμε το πεπερασμένο σώμα $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/x^4+x+1$, και έστω $\alpha \in \mathbb{F}_{2^4}$ πρωταρχική ρίζα του x^4+x+1.
α) Να βρεθεί η παραγοντοποίηση του πολυωνύμου x^4+x+1 στο $\mathbb{F}_{2^4}$.
β) Να βρεθεί το αντίστροφο στοιχείο ως προς τον πολλαπλασιασμό του στοιχείου $\alpha^3+\alpha^2$.
γ) Να δειχθεί ότι το στοιχείο α^7 είναι ρίζα του πολυωνύμου x^4+x^3+1.

Θέμα 2 (1 μονάδα)
α) Να βρεθούν όλα τα υποσώματα των πεπερασμένων σωμάτων (i) $\mathbb{F}_{2^{32}}$ και (ii) $\mathbb{F}_{3^{42}}$ και να κατασκευασθεί το πλέγμα υποσωμάτων τους.
β) Να βρεθεί το πλήθος των (i) ανάγωγων και (ii) των πρωταρχικών πολυωνύμων βαθμού 6 πάνω στο $\mathbb{F}_2$.

Θέμα 3 (2 μονάδες)
α) Χρησιμοποιώντας το κριτήριο που βασίζεται στον αλγόριθμο του Berlekamp να αποδειχθεί ότι το πολυώνυμο $f(x) = x^5+2\,x+1$ είναι ανάγωγο στο $\mathbb{F}_3[x]$.
β) Χρησιμοποιώντας τον αλγόριθμο του Berlekamp να παραγοντοποιηθεί σε γινόμενα ανάγωγων πολυωνύμων το $f(x) = x^4+x^3+x^2+1$ στο $\mathbb{F}_2[x]$.

Θέμα 4 (1 μονάδα)
α) Χρησιμοποιώντας τα κυκλοτομικά πολυώνυμα να παραγοντοποιηθεί σε γινόμενο ανάγωγων πολυωνύμων το x^8-1 στο $\mathbb{F}_3[x]$, δεδομένου ότι τα μόνα (μονικά) ανάγωγα πολυώνυμα βαθμού 2 στο $\mathbb{F}_3[x]$ είναι τα: x^2+1, x^2+x+2, $x^2+2\,x+2$.
β) Να διερευνηθεί αν τα παρακάτω κυκλοτομικά πολυώνυμα είναι ανάγωγα ή όχι πάνω στο δοσμένο σώμα:

$$\text{(i)}\quad Q_6(x) \text{ στο } \mathbb{F}_5\,, \quad \text{(ii)}\quad Q_{11}(x) \text{ στο } \mathbb{F}_3\,,$$

και να βρεθεί το πλήθος και ο βαθμός των ανάγωγων πολυωνύμων που αναλύονται (αν αναλύονται).

Θέμα 5 (1 μονάδα) Να υπολογιστούν τα παρακάτω κυκλοτομικά πολυώνυμα:

$$\text{(i) } Q_{20}(x)\,, \qquad \text{(ii) } Q_{25}(x)\,, \qquad \text{(iii) } Q_{32}(x)\,, \qquad \text{(iv) } Q_{36}(x)\,.$$

Θέμα 6 (2 μονάδες) Θεωρούμε δυαδική κωδικο-συνάρτηση $f : B^3 \to B^7$ με γεννήτορα πίνακα

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

α) Να βρεθούν οι κωδικολέξεις και το πλήθος των λαθών που εντοπίζει και διορθώνει ο κώδικας.
β) Να βρεθεί ο πίνακας συνδρόμων-πλευρικών οδηγών της f.
γ) Ένα μήνυμα κωδικοποιείται με την εξής αντιστοιχία

000 _	001 A	010 E	100 O
011 S	101 T	110 M	111 N

και λαμβάνουμε 0011100, 0001101, 1111100. Να αποκωδικοποιηθεί το μήνυμα.

Θέμα 7 (2 μονάδες) Το πολυώνυμο x^9-1 παραγοντοποιείται στο $\mathbb{F}_2$ ως εξής

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

α) Να βρεθεί το πολυώνυμο-γεννήτορας του ελάχιστου δυαδικού κυκλικού κώδικα μήκους 9 που περιέχει την κωδικολέξη 001000001.
β) Έστω C ο δυαδικός κυκλικός κώδικας μήκους 9 με πολυώνυμο γεννήτορα το $g(x) = 1+x^3+x^6$. Να βρεθεί ο γεννήτορας πίνακας του C.
γ) Μια λέξη κωδικοποιείται με τον C και λαμβάνεται ως $w = 000001001$. Να αποκωδικοποιηθεί η λέξη w, δεδομένου ότι ο C εντοπίζει 2-λάθη και διορθώνει 1-λάθος.

Εύχομαι κάθε επιτυχία

Ενδεικτικές απαντήσεις των θεμάτων

Θέμα 1

α) Μας ζητείται να παραγοντοποιήσουμε το (ελάχιστο) πολυώνυμο $p(x) = x^4 + x + 1$ στο πεπερασμένο σώμα $\mathbb{F}_{2^4}$ ως την επέκταση $\mathbb{F}_2[x]/p(x)$ του ελάχιστου υποσώματος $\mathbb{F}_2$.

Αφού $\alpha \in \mathbb{F}_{2^4}$ πρωταρχική ρίζα του $p(x)$ ($\alpha^{15} = 1$), μπορούμε να αναπαραστήσουμε τα στοιχεία του $\mathbb{F}_{2^4}$ στην μορφή $f(a)$ όπου $f(x)$ είναι τα $2^4 = 16$ πολυώνυμα στο $\mathbb{F}_2$ βαθμού $d \leq 3$, και

$$\mathbb{F}_{2^4} = \{0, 1, \alpha, \alpha^2, \ldots \alpha^{14}\}\,.$$

Έστω $\Phi : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ ο αυτομορφισμός Frobenius με τύπο $\Phi(x) = x^2$. Η παραγοντοποίηση του $p(x)$ είναι η εξής

$$p(x) = \big(x - \alpha\big)\big(x - \Phi(\alpha)\big)\big(x - \Phi^2(\alpha)\big)\big(x - \Phi^3(\alpha)\big) = \big(x - \alpha\big)\big(x - \alpha^2\big)\big(x - \alpha^4\big)\big(x - \alpha^8\big)\,. \tag{1}$$

Αφού $p(\alpha) = 0$ τότε

$$\alpha^4 + \alpha + 1 = 0 \Rightarrow \alpha^4 = -\alpha - 1 \Rightarrow \alpha^4 = \alpha + 1\,, \tag{2}$$

($-1 \equiv 1 \mod 2$), και

$$\alpha^8 = (\alpha^4)^2 = (\alpha + 1)^2 = \alpha^2 + 1\,, \qquad (\equiv \mod 2) \tag{3}$$

Χρησιμοποιώντας τις σχέσεις (2) και (3), η (1) γίνεται

$$p(x) = \big(x + \alpha\big)\big(x + \alpha^2\big)\big(x + \alpha + 1\big)\big(x + \alpha^2 + 1\big)\,.$$

β) Μας ζητείται να βρούμε το αντίστροφο στοιχείο ως προς τον πολλαπλασιασμό του στοιχείου $\alpha^3 + \alpha^2$. Έστω $g(x) = x^3 + x^2$. Αφού το $p(x)$ είναι πρωταρχικό πολυώνυμο τότε

$$\text{μ.κ.δ.}(p(x), g(x)) = 1\,,$$

και αρκεί να βρούμε από τον αλγόριθμο του Ευκλείδη τα $a(x), b(x)$ τέτοια ώστε

$$1 = a(x)\,p(x) + b(x)\,g(x)$$

Έχουμε

$$\begin{aligned} x^4 + x + 1 &= (x+1)(x^3 + x^2) + (x^2 + x + 1) \\ x^3 + x^2 &= x(x^2 + x + 1) + x \\ x^2 + x + 1 &= x(x+1) + 1\,. \end{aligned}$$

Οπότε

$$1 = (x^2 + x + 1)\,p(x) + (x^2 + x)\,g(x)$$

και παίρνοντας $\mod p(x)$ έχουμε

$$[1]_{p(x)} = [x^2 + x]_{p(x)}\,[g(x)]_{p(x)}$$

συνεπώς το αντίστροφο του στοιχείου $\alpha^3 + \alpha^2$ είναι το $\alpha^3 + \alpha$.

γ) Έστω $h(x) = x^4 + x^3 + 1$. Μας ζητείται να δείξουμε ότι το στοιχείο α^7 είναι μια ρίζα του $h(x)$. Αρκεί να δείξουμε ότι $h(\alpha^7) = 0$. Πράγματι, έχουμε

$$\begin{aligned} h(\alpha^7) &= (\alpha^7)^4 + (\alpha^7)^3 + 1 = \alpha^{28} + \alpha^{21} + 1 = \alpha^{15}\,\alpha^{13} + \alpha^{15}\,\alpha^6 + 1 = \alpha^{13} + \alpha^6 + 1 \\ &= \alpha^9\,\alpha^4 + \alpha^2\,\alpha^4 + 1 = (\alpha^3 + \alpha)(\alpha + 1) + \alpha^2(\alpha + 1) + 1 \\ &= \alpha^4 + \alpha^3 + \alpha^2 + \alpha + \alpha^3 + \alpha^2 + 1 = \alpha^4 + \alpha + 1 = 0 \end{aligned}$$

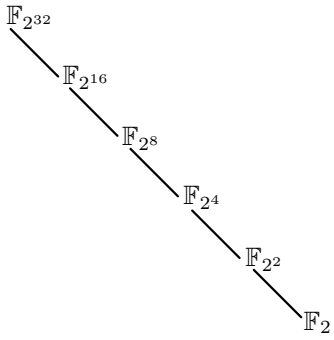
Θέμα 2

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 $n = 32$ είναι $1, 2, 4, 8, 16, 32$. Συνεπώς τα υποσώματα του $\mathbb{F}_{2^{18}}$ είναι τα :

$$\mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^4}, \mathbb{F}_{2^8}, \mathbb{F}_{2^{16}}, \mathbb{F}_{2^{32}}$$

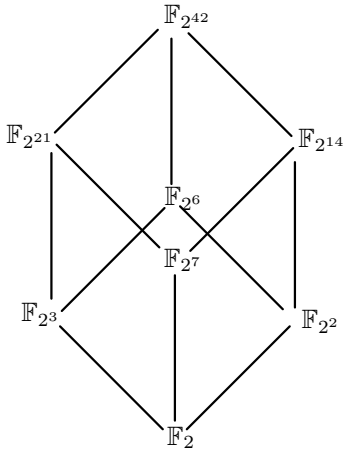
Το πλέγμα των υποσωμάτων δίνεται σχηματικά από το παρακάτω



(ii) Οι διαιρέτες του $n = 42$ είναι $1, 2, 3, 6, 7, 14, 21, 42$. Συνεπώς τα υποσώματα του $\mathbb{F}_{3^{40}}$ είναι τα :

$$\mathbb{F}_3, \mathbb{F}_{3^2}, \mathbb{F}_{3^3}, \mathbb{F}_{3^6}, \mathbb{F}_{3^7}, \mathbb{F}_{3^{14}}, \mathbb{F}_{3^{21}}, \mathbb{F}_{3^{42}}$$

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

$$\begin{aligned} \Pi_2(6) &= \frac{1}{6}\sum_{d|6} \mu(\frac{6}{d})2^d = \frac{1}{6}(\mu(6)2^1 + \mu(3)2^2 + \mu(2)2^3 + \mu(1)2^6) = \frac{1}{8}((-1)^2\,2^1 + (-1)\,2^2 + (-1)2^3 + 2^6) \\ &= \frac{1}{6}(2^6 + 2 - 2^3 - 2^2) = \frac{54}{6} = 9 \end{aligned}$$

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

$$\begin{aligned} \frac{\varphi(2^6 - 1)}{6} &= \frac{\varphi(64 - 1)}{6} = \frac{\varphi(63)}{8} = \frac{\varphi(3^2 \cdot 7)}{6} = \frac{\varphi(3^2)\varphi(7)}{6} = \frac{3(3-1)(7-1)}{6} \\ &= \frac{6 \cdot 6}{6} = 6 \end{aligned}$$

Συνεπώς υπάρχουν 9 ανάγωγα πολυώνυμα βαθμού 6 πάνω στο $\mathbb{F}_2$, από τα οποία τα 6 είναι πρωταρχικά.

Θέμα 3

α) Μια βάση του διανυσματικού χώρου $\mathbb{F}_3[x]/f(x)$ όπου $f(x) = x^5 + 2\,x + 1$ είναι η $e = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$, όπου $\alpha = [x]_f$. Έχουμε την γραμμική απεικόνιση (αυτομορφισμό Frobenius) $\Phi(a) = a^3$. Εφαρμόζουμε την απεικόνιση Φ στην βάση e και έχουμε

$$\begin{aligned}
\Phi(1) &= 1 \\
\Phi(\alpha) &= \alpha^3 \\
\Phi(\alpha^2) &= \alpha^6 = \alpha\,\alpha^5 = \alpha^2 + 2\alpha \qquad (\alpha^5 = \alpha + 2) \\
\Phi(\alpha^3) &= \alpha^9 = \alpha^3\alpha^6 = \alpha^3(\alpha^2 + 2\alpha) = \alpha^5 + 2\alpha^4 = 2\alpha^4 + \alpha + 2 \\
\Phi(\alpha^4) &= \alpha^{12} = \alpha^6\alpha^6 = (\alpha^2 + 2\alpha)(\alpha^2 + 2\alpha) = \alpha^4 + 4\,\alpha^3 + 4\,\alpha^2 = \alpha^4 + \alpha^3 + \alpha^2 \qquad (\equiv \mod 3)
\end{aligned}$$

οπότε ο πίνακας της Φ στην βάση e είναι ο

$$[\Phi]_{\{e\}} = \begin{array}{c} \\ 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix} \end{array}$$

Σύμφωνα με το κριτήριο που βασίζεται στον αλγόριθμο του Berlekamp, 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

$$\begin{pmatrix} 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{array}{r} x_1 + 2x_4 = 0 \\ 2x_3 + x_4 = 0 \\ x_3 + x_5 = 0 \\ x_2 + x_5 = 0 \\ 2x_4 + x_5 = 0 \end{array} \Rightarrow \begin{array}{l} x_1 = 2x_4 \\ x_2 = 2x_4 \\ x_3 = 2x_4 \\ x_4 = 2x_4 \\ x_5 = \ x_4 \end{array} \Rightarrow \begin{array}{l} x_1 = 0 \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = 0 \\ x_5 = 0 \end{array}$$

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

$$\begin{pmatrix} 0 & 0 & 0 & 2 & 0 \\ 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{array}{r} 2x_4 = 0 \\ 2x_2 + 2x_3 + x_4 = 0 \\ x_5 = 0 \\ x_2 + 2x_4 + x_5 = 0 \\ 2x_4 = 0 \end{array} \Rightarrow \begin{array}{l} x_1 \in \mathbb{F}_3 \text{ αυθαίρετο} \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = 0 \\ x_5 = 0 \end{array}$$

άρα $\ker(\Phi - I) = \mathbb{F}_3$ και συνεπώς το $f(x) = x^5 + 2x + 1$ είναι ανάγωγο πάνω στο $\mathbb{F}_3$.

β) Μια βάση του διανυσματικού χώρου $\mathbb{F}_3[x]/f(x)$ όπου $f(x) = x^4 + x^3 + x^2 + 1$ 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

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

οπότε ο πίνακας της Φ στην βάση e είναι ο

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

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

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

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

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

και $\ker(\Phi - I) = \{(1,0,0,0), (0,1,0,1)\}$. Το διάνυσμα $(0,1,0,1)$ αντιστοιχεί στο πολυώνυμο $h(x) = x + x^3$. Από τον αλγόριθμο του Berlekamp γνωρίζουμε ότι τα πολυώνυμα μ.κ.δ$(f(x), h(x))$ και μ.κ.δ$(f(x), h(x) - 1)$ είναι ανάγωγοι παράγοντες του $f(x)$. Εκτελώντας τον Ευκλείδιο αλγόριθμο διαίρεσης για την εύρεση μ.κ.δ. πολυωνύμων βρίσκουμε ότι:

$$\begin{aligned} \text{μ.κ.δ}(f(x), h(x)) &= x + 1 \\ \text{μ.κ.δ}(f(x), h(x) - 1) &= x^3 + x + 1 \end{aligned}$$

οπότε

$$x^4 + x^3 + x^2 + 1 = (x+1)(x^3 + x + 1)$$

είναι η ανάλυση σε ανάγωγα πολυώνυμα του $f(x)$.

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

$$\begin{aligned} x^4 + x^3 + x^2 + 1 &= (x+1)(x^3 + x) + (x+1) \\ x^3 + x &= (x^2 + x)(x+1) \end{aligned}$$

Οπότε μ.κ.δ$(f(x), h(x)) = x + 1$.

Για το μ.κ.δ$(f(x), h(x) + 1)$

$$x^4 + x^3 + x^2 + 1 = (x+1)(x^3 + x + 1)$$

Οπότε μ.κ.δ$(f(x), h(x) + 1) = x^3 + x + 1$

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 $\mathbb{F}_3$ και $n = 8$ και $3 \nmid 8$. Οι διαιρέτες του 8 είναι $1, 2, 4, 8$, οπότε έχουμε

$$x^8 - 1 = Q_1(x)\, Q_2(x)\, Q_4(x)\, Q_8(x)$$

Από τη θεωρία γνωρίζουμε ότι

$$\begin{aligned} Q_1(x) &= x - 1 = x + 2 \qquad (\equiv \mod 3) \\ Q_2(x) &= x + 1 \end{aligned}$$

Προφανώς τα πολυώνυμα $Q_1(x), Q_2(x)$ είναι ανάγωγα πάνω στο $\mathbb{F}_3$. Αρκεί να υπολογίσουμε τα πολυώνυμα $Q_4(x), Q_8(x)$ και να βρούμε αν είναι ανάγωγα ή όχι. Στην περίπτωση που δεν είναι ανάγωγα θα πρέπει με κάποιον τρόπο να τα 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

$$Q_4(x) = (x^4 - 1)^{\mu(1)}\, (x^2 - 1)^{\mu(2)} (x - 1)^{\mu(4)}$$

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

$$Q_4(x) = \frac{x^4 - 1}{x^2 - 1} = \frac{(x^2 - 1)(x^2 + 1)}{x^2 - 1} = x^2 + 1$$

Αλλιώς, από ιδιότητα των κυκλοτομικών πολυωνύμων

$$Q_4(x) = Q_{2^2}(x) = Q_2(x^2) = x^2 + 1$$

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 $Q_4(x)$ ότι

$$\varphi(4) = \varphi(2^2) = 2(2-1) = 2$$

Επιπλέον

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

άρα $o_4(3) = 6 = \varphi(4)$ και συνεπώς το κυκλοτομικό πολυώνυμο $Q_4(x)$ είναι ανάγωγο πάνω στο $\mathbb{F}_3$. Αλλιώς, $Q_4(0) = 1$, $Q_4(1) = Q_4(2) = 1$ που σημαίνει το $Q_4(x)$ δεν έχει ρίζες στο $\mathbb{F}_3$ και συνεπώς είναι ανάγωγο στο $\mathbb{F}_3$.

Για το $Q_8(x)$

$$Q_8(x) = (x^8-1)^{\mu(1)}\,(x^4-1)^{\mu(2)}(x^2-1)^{\mu(4)}\,(x-1)^{\mu(8)}$$

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

$$Q_8(x) = \frac{x^8-1}{x^4-1} = \frac{(x^4-1)(x^4+1)}{x^4-1} = x^4+1$$

Αλλιώς, από ιδιότητα των κυκλοτομικών πολυωνύμων

$$Q_8(x) = Q_{2^3}(x) = Q_2(x^4) = x^4+1$$

Εδώ έχουμε για τον βαθμό του $Q_8(x)$ ότι

$$\varphi(8) = \varphi(2^3) = 2^2(2-1) = 4$$

Επιπλέον

$$\begin{aligned} 3 &\equiv 3 \mod 8 \\ 3^2 &\equiv 1 \mod 8 \end{aligned}$$

άρα $o_8(3) = 2 \neq 4 = \varphi(8)$ και συνεπώς το κυκλοτομικό πολυώνυμο $Q_8(x)$ είναι δεν ανάγωγο πάνω στο $\mathbb{F}_3$, και αναλύεται σε 2 ανάγωγα πολυώνυμα ίδιου βαθμού 2. Από τα δεδομένα του θέματος εύκολα συμπεραίνουμε ότι

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

Τελικά έχουμε ότι η ανάλυση του x^8-1 σε ανάγωγα πολυώνυμα πάνω στο $\mathbb{F}_3$ είναι

$$x^8-1 = (x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2\,x+2)\,.$$

β) 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 $Q_6(x)$ στο $\mathbb{F}_5$ έχουμε:

$$\varphi(6) = \varphi(2\cdot 3) = \varphi(2)\varphi(3) = (2-1)(3-1) = 2$$

Επιπλέον

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

Άρα $o_6(3) = \varphi(6) = 2$ και συνεπώς το $Q_6(x)$ είναι ανάγωγο πάνω στο $\mathbb{F}_5$.
(ii) Για το $Q_{11}(x)$ στο $\mathbb{F}_3$ έχουμε:

$$\varphi(11) = (11-1) = 10$$

Επιπλέον

$$\begin{aligned} 3 &\equiv 3 \mod 11 \\ 3^2 &\equiv 9 \mod 11 \\ 3^3 &\equiv 5 \mod 11 \\ 3^2 &\equiv 4 \mod 11 \\ 3^5 &\equiv 1 \mod 11 \end{aligned}$$

Άρα $o_{11}(3) = 5 \neq 10 = \varphi(11)$. Συνεπώς το $Q_{11}(x)$ δεν είναι ανάγωγο πάνω στο $\mathbb{F}_3$ και αναλύεται σε 2 ανάγωγα πολυώνυμα ίδιου βαθμού 5.

Θέμα 5

Για το υπολογισμό των κυκλοτομικών πολυωνύμων έχουμε:

(i)

$$Q_{20}(x) = Q_{2^2\cdot 5}(x) = Q_{2\cdot 5}(x^2) = Q_{10}(x^2)$$

Αρκεί να υπολογίσουμε το $Q_{10}(x)$. Από τον ορισμό των $Q_n(x)$ έχουμε

$$\begin{aligned} Q_{10}(x) &= (x^{10}-1)^{\mu(1)}\,(x^2-1)^{\mu(5)}(x^5-1)^{\mu(2)}(x-1)^{\mu(10)} = \frac{(x^{10}-1)(x-1)}{(x^2-1)(x^5-1)} = \frac{(x^5-1)(x^5+1)(x-1)}{(x-1)(x+1)(x^5-1)} \\ &= \frac{x^5+1}{x+1} = \frac{(x+1)(x^4-x^3+x^2-x+1)}{x+1} = x^4-x^3+x^2-x+1 \end{aligned}$$

Συνεπώς, έχουμε

$$Q_{20}(x) = Q_{10}(x^2) = x^8 - x^6 + x^4 - x^2 + 1$$

(ii)

$$Q_{25}(x) = Q_{5^2}(x) = Q_5(x^5)$$

Αρκεί να υπολογίσουμε το $Q_{10}(x)$. Από τον ορισμό των $Q_p(x)$ με p πρώτο έχουμε

$$Q_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

Συνεπώς,

$$Q_5(x) = x^4 + x^3 + x^2 + x + 1$$

και

$$Q_{25}(x) = Q_5(x^5) = x^{20} + x^{15} + x^{10} + x^5 + 1$$

(iii)

$$Q_{32}(x) = Q_{2^5}(x) = Q_2(x^{2^5-2^4}) = Q_2(x^{16}) = x^{16} + 1$$

(iv)

$$Q_{36}(x) = Q_{6^2}(x) = Q_6(x^6)$$

Εύκολα βρίσκουμε ότι $Q_6(x) = x^2 - x + 1$, κι έτσι

$$Q_{36}(x) = x^{12} - x^6 + 1$$

Θέμα 6

α) Θεωρούμε την δυαδική κωδικο-συνάρτηση $f : B^3 \to B^7$ με γεννήτορα πίνακα

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

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

$$\begin{array}{cc} 000 & 0000000 \\ 001 & 0010111 \\ 010 & 0101011 \\ 011 \xrightarrow{f} & 0111100 \\ 100 & 1001101 \\ 101 & 1011010 \\ 110 & 1100110 \\ 111 & 1110001 \end{array}$$

Επειδή $\min \mathrm{d} = 4$, ο κώδικας εντοπίζει $4-1 = 2$-λάθη και διορθώνει $\left[\frac{4-1}{2}\right] = 1$-λάθη.

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

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

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

σύνδρομα	πλευρικοί οδηγοί
0000	0000000
1101	1000000
1011	0100000
0111	0010000
1000	0001000
0100	0000100
0010	0000010
0001	0000001
0011	0000011
0101	0000101
1001	0001001
0110	0010001
1010	0100001
1100	1000001
1111	1000010
1110	0001101

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) συνεχίζουμε με λέξεις ελάχιστου βάρους 2 κοκ. Οπότε έχουμε ένα πλήρη πίνακα σύνδρομων-πλευρικών οδηγών.

γ) Το μήνυμα που λαμβάνουμε είναι 0011100, 0001101, 1111100. 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 $w_1 = (0,0,1,1,1,0,0)$, $w_2 = (0,0,0,1,1,0,1)$, $w_3 = (1,1,1,1,1,0,0)$ και έχουμε

σύνδρομο		πλευρικός οδηγός	διορθωμένη λέξη	κωδικολέξη	αποκωδ/μένο μήνυμα
$w_1H = (1,0,1,1)$	$\rightarrow$	$e_1 = (0,1,0,0,0,0,0)$	$w_1 + e_1 = (0,1,1,1,1,0,0)$	0111100	011 S
$w_2H = (1,1,0,1)$	$\rightarrow$	$e_2 = (1,0,0,0,0,0,0)$	$w_2 + e_2 = (1,0,0,1,1,0,1)$	1001101	100 O
$w_3H = (1,1,0,1)$	$\rightarrow$	$e_3 = (1,0,0,0,0,0,0)$	$w_3 + e_3 = (0,1,1,1,1,0,0)$	0111100	011 S

Θέμα 7

α) Μας ζητείται να βρούμε τον ελάχιστο κυκλικό κώδικα μήκους 9 που περιέχει την κωδικολέξη 001000001. Θέτουμε $f(x) = x^9 - 1$, και $h(x) = x^2 + x^8$, το πολυώνυμο που αντιστοιχεί στην κωδικολέξη 001000001. 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

$$\begin{aligned} x^9 - 1 = x^9 + 1 \quad (\equiv \mod 2) &= x(x^8 + x^2) + (1 + x^3) \\ (x^8 + x^2) &= (x^5 + x^2)(1 + x^3) \end{aligned}$$

Συνεπώς $g(x) = 1 + x^3$ είναι το ζητούμενο πολυώνυμο-γεννήτορας.

β) Έχουμε έναν κυκλικό κώδικα μήκους 9 με πολυώνυμο-γεννήτορα $g(x) = 1 + x^3 + x^6$, οπότε

$$C : B^3 \to B^9$$

και ο κυκλικός κώδικας παράγεται από τον πίνακα

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

γ) Η λέξη που λήφθηκε είναι η $w = 000001001$ η οποία αντιστοιχεί στο πολυώνυμο $w(x) = x^5 + x^8$. Παρατηρούμε ότι

$$x^8 + x^5 = x^2(1 + x^3 + x^6) + x^2$$

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

$$s(x) = w(x) \mod g(x) = x^2$$

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

$$e(x) = x^{9-0}s(x) \mod (x^9 + 1) = x^{11} \mod (x^9 + 1) = x^2$$

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

$$\widetilde{w}(x) = w(x) + e(x) = x^2 + x^5 + x^8 = x^2\, g(x)$$

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

$$x^2\, g(x)/g(x) = x^2$$

που αντιστοιχεί στη λέξη $001 \in B^3$.