Ασκήσεις Εφαρμοσμένης Άλγεβρας

1 Να υπολογισθεί ο μέγιστος κοινός διαιρέτης d των $f(x) = x^7 + x^6 + x^2 + x + 1$ και $g(x) = x^7 + x^5 + x^4 + x^2 + 1$ στο $\mathbb{F}_2[x]$ καθώς και τα $\lambda, \mu \in \mathbb{F}_2[x]$, τέτοια που $d = \lambda\, f + \mu\, g$.

2 Να δειχθεί ότι το $f(x) = x^5 - x + 1$ είναι ένα ανάγωγο πολυώνυμο στο $\mathbb{F}_3[x]$. Υποθέτοντας ότι το $f(x)$ είναι πρωταρχικό πολυώνυμο επιχειρηματολογήστε για ότι το $\mathbb{F}_3[x]/f(x)$ είναι ένα σώμα με 243 στοιχεία. Έστω $\alpha = [x]$. Βρείτε ένα στοιχείο $\gamma \in \mathbb{F}_3[x]/f(x)$ τέτοιο που $\alpha\,\gamma = 1$ στο $\mathbb{F}_3[x]/f(x)$.

3 Να βρεθούν όλα τα υποσώματα του $\mathbb{F}_{2^{24}}$, και να κατασκευασθεί το πλέγμα υποσωμάτων.

4 Να κατασκευασθεί ο πίνακας του σώματος $\mathbb{F}_9 = \mathbb{F}_3[x]/x^2 + 2\,x + 2$ και να βρεθούν τα ελάχιστα πολυώνυμα των στοιχείων του. Αν $\alpha \in \mathbb{F}_9$ να βρεθεί ένα στοιχείο του $\mathbb{F}_9$ το οποίο είναι ρίζα του πολυωνύμου $x^2 + 1$.

5 Να δειχθεί ότι υπάρχουν 440 μονικά ανάγωγα πολυώνυμα βαθμού 3 στο $\mathbb{F}_{11}[x]$, και 804076 βαθμού 6 στο $\mathbb{F}_{13}[x]$. Σε κάθε περίπτωση πόσα από αυτά είναι πρωταρχικά πολυώνυμα;

6 Να βρεθούν οι παραγοντοποιήσεις σε γινόμενα ανάγωγων πολυωνύμων των $x^{2^2} - x \in \mathbb{F}_2[x]$ και $x^{3^2} - x \in \mathbb{F}_3[x]$.

7 Χρησιμοποιώντας το κριτήριο που βασίζεται στον αλγόριθμο του Berlekamp να δειχθεί ότι το πολυώνυμο $f(x) = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$, είναι ανάγωγο.

8 Χρησιμοποιώντας το κριτήριο που βασίζεται στον αλγόριθμο του Berlekamp να δειχθεί ότι το πολυώνυμο $f(x) = x^6 + x^3 + 1 \in \mathbb{F}_2[x]$, είναι ανάγωγο.

9 Χρησιμοποιώντας τον αλγόριθμο του Berlekamp να βρεθεί μια παραγοντοποίηση σε γινόμενα ανάγωγων πολυωνύμων του $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_3[x]$.

10 Χρησιμοποιώντας τον αλγόριθμο του Berlekamp να βρεθεί μια παραγοντοποίηση σε γινόμενα ανάγωγων πολυωνύμων του $f(x) = x^6 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$.