

Ασκήσεις Πεπερασμένων Σωμάτων και κρυπτογραφίας
2 Φυλλάδιο

Παράδοση 30 Απριλίου 2012

1. Να υπολογιστεί το πλήθος των αναγώγων πολυωνύμων βαθμού 24 πάνω από ένα σώμα με q το πλήθος στοιχείων.
2. Για κάθε διαιρέτη k του $2^4 - 1 = 15$ να υπολογίσουν οι πρωταρχικές k ρίζες του 1 σε κατάληλες επεκτάσεις του σώματος με 2 στοιχεία. Υπόδειξη: Το $x^4 + x + 1$ είναι ένα πρωταρχικό πολυώνυμο.
3. Να υπολογιστούν τα κυκλοτομικά πολυώνυμα βαθμού μέχρι 12 πάνω από ένα σώμα που έχει χαρακτηριστική $p > 12$.
4. Να αποδειχτεί ότι τα κυκλοτομικά πολυώνυμα ενός σώματος με p^h στοιχεία έχουν συντελεστές που ανήκουν στο σώμα με p το πλήθος στοιχείων.
5. Να αποδειχτεί ότι το n κυκλοτομικό πολυώνυμο δίνεται από τον τύπο

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

όπου μ είναι η πολλαπλασιαστική συνάρτηση του Möbius

$$\mu(m) = \begin{cases} 1 & \text{αν } m = 1 \\ (-1)^k & \text{αν το } m \text{ διασπάται σε γινόμενο } k \text{ διαφορετικών πρώτων} \\ 0 & \text{αν το } m \text{ διαιρείται με τετράγωνο} \end{cases}$$