ΚΩΔΙΚΟΠΟΙΗΣΗ
ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ #1

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

(1) Έστω το πολυώνυμο $f = X^4 + X + 1 \in \mathbb{F}_2[X]$.
   (α′) Δείξτε ότι το f είναι ανάγωγο πάνω από το $\mathbb{F}_2$.
   (β′) Αν α είναι μια ρίζα του f, υπολογίστε την τάξη των στοιχείων α και $\alpha+1$ στην ομάδα $\mathbb{F}_{16}^*$.
   (γ′) Εκφράστε όλους τους γεννήτορες της πολ/κης ομάδας ως προς τη βάση $\{1, \alpha, \alpha^2, \alpha^3\}$.

(2) Κατασκευάστε την επέκταση $\mathbb{F}_{125}|\mathbb{F}_5$, χρησιμοποιώντας μια ρίζα, β, του πολυωνύμου $g = X^3 + X + 1$. Εκφράστε τα στοιχεία $\beta, \beta^5, \beta^{25}$ ως προς τη βάση $\{1, \beta, \beta^2\}$. Είναι γραμμικά ανεξάρτητα;

(3) (α′) Υπολογίστε τα κυκλοτομικά σύμπλοκα του 2 modulo 31.
   (β′) Αν α είναι μια ρίζα του ανάγωγου $X^5 + X^2 + 1 \in \mathbb{F}_2[X]$, υπολογίστε τα ελάχιστα πολυώνυμα των στοιχείων $\alpha, \alpha^4, \alpha^5$.
   (γ′) Αναλύστε το πολυώνυμο $X^{31} - 1$ σε ανάγωγους παράγοντες πάνω από το $\mathbb{F}_2$.