

M2426 – Εφαρμοσμένη Άλγεβρα

Θεόδουλος Γαρεφαλάκης

March 23, 2017

1. Έστω p περιττός πρώτος αριθμός, $n \in \mathbb{N}$ και $q = p^n$. Ορίζουμε $(\mathbb{F}_q^*)^2 = \{a^2 : a \in \mathbb{F}_q\}$.
 - (a) Δείξτε ότι η απεικόνιση $\theta : \mathbb{F}_q^* \rightarrow \mathbb{F}_q^*$ με $\theta(a) = a^2$ είναι ομομορφισμός ομάδων.
 - (b) Υπολογίστε τον πυρήνα και την εικόνα του θ .
 - (c) Δείξτε ότι $|(\mathbb{F}_q^*)^2| = (q - 1)/2$.
2. Έστω $n \in \mathbb{N}$ και $q = 2^n$. Δείξτε ότι $(\mathbb{F}_q^*)^2 = \mathbb{F}_q^*$.
3. Έστω p πρώτος αριθμός, $n \in \mathbb{N}$ και $q = p^n$. Δείξτε ότι κάθε στοιχείο του \mathbb{F}_q γράφεται ως άθροισμα δύο τετραγώνων, δηλαδή για κάθε $c \in \mathbb{F}_q$ υπάρχουν $a, b \in \mathbb{F}_q$ τέτοια ώστε $c = a^2 + b^2$.
Υπόδειξη: Δείξτε ότι τα σύνολα $\{c - a^2 : a \in \mathbb{F}_q\}$ και $\{b^2 : b \in \mathbb{F}_q\}$ έχουν μη κενή τομή.
4. Αναλύστε σε ανάγωγους παράγοντες το πολυώνυμο $X^{30} - 1 \in \mathbb{F}_3[X]$.
5. Έστω ℓ_1, ℓ_2 διακεκριμένοι περιττοί πρώτοι αριθμοί, τέτοιοι ώστε $\text{μκδ}(\ell_1 - 1, \ell_2 - 1) = 2$ και $\text{ord}_{\ell_i}(2) = \ell_i - 1$ για $i = 1, 2$. Υπολογίστε το πλήθος των μονικών αναγώγων που εμφανίζονται στην ανάλυση του $X^{\ell_1 \ell_2} - 1 \in \mathbb{F}_2[X]$.
6. Έστω p πρώτος αριθμός, $n \in \mathbb{N}$ και $q = p^n$. Συμβολίζουμε με I_n το σύνολο των μονικών αναγώγων πολυωνύμων του $\mathbb{F}_p[X]$.
 - (a) Έστω $n > 1$ και $f \in I_n$. Δείξτε ότι όλες οι ρίζες του f έχουν την ίδια τάξη στην ομάδα \mathbb{F}_q^* .
 - (b) Δείξτε ότι αν α είναι γεννήτορας της ομάδας \mathbb{F}_q^* , τότε $\min(\alpha, \mathbb{F}_p) \in I_n$.
 - (c) Υπολογίστε το πλήθος των στοιχείων του συνόλου

$$J_n = \{f \in I_n : \text{Κάθε ρίζα του } f \text{ έχει τάξη } q - 1\}.$$