

Ασκήσεις Πεπερασμένων Σωμάτων και κρυπτογραφίας

1 Φυλλάδιο

Παράδοση 3 Απριλίου 2012

1. Να υπολογιστεί ένας γεννήτορας των κυκλικών ομάδων $\mathbb{F}_{13}$, $\mathbb{F}_{23}$.
2. Να λυθεί η διαφορική εξίσωση (!) $\frac{d}{dx}f = 0$ όπου οι επιτρεπτές λύσεις $f \in k[x]$.
3. Θα λέμε ότι ένα πολυώνυμο είναι προσθετικό αν και μόνο αν είναι της μορφής

$$f(x) = \sum_{\nu=0}^n a_{\nu} x^{p^{\nu}}.$$

Αποδείξτε ότι ένα πολυώνυμο είναι προσθετικό αν και μόνο αν οι ρίζες του αποτελούν ένα $\mathbb{F}_p$ διανυσματικό χώρο.

4. Αποδείξτε ότι στην χαρακτηριστική 0 τα ανάγωγα πολυώνυμα δεν έχουν πολλαπλές ρίζες. Τι μπορεί να συμβεί στην πεπερασμένη χαρακτηριστική;
5. Αποδείξτε ότι σε ένα αντιμεταθετικό δακτύλιο με μονάδα R τα παρακάτω είναι ισοδύναμα: Ένα ιδεώδες I είναι πρώτο αν και μόνο αν R/I ακαιρέα περιοχή. Ένα ιδεώδες I είναι μέγιστο αν και μόνο αν R/I είναι σώμα. Αποδείξτε ότι αν το $f(x)$ είναι ένα ανάγωγο πολυώνυμο τότε το $K[x]/\langle f \rangle$ είναι σώμα.
6. Αποδείξτε ότι στους δακτυλίους $\mathbb{Z}$ και $F[X]$, όπου F σώμα ένα ιδεώδες είναι πρώτο αν και μόνο αν είναι μέγιστό. Ισχύει αυτό γενικά σε κάθε αντιμεταθετικό δακτύλιο;