Πεπερασμένα Σώματα και Κρυπτογραφία

Εξετάσεις 14 Ιουνίου 2016

Θεμα 1.

(1) Να υπολογιστεί ο μέγιστος κοινός διαιρέτης των αριθμών 12839 και 1728 και να εκφραστεί ως γραμμικός συνδιασμός με συντεστές ακεραίους αυτών.
(2) Πότε μια συνάρτηση είναι πολλαπλασιαστική; Να δοθεί ο ορισμός. Να αποδειχθεί ότι η ϕ συνάρτηση του Euler είναι πολλαπλασιατική.
(3) Δίνεται ένας πρώτος ο οποίος είναι $p \equiv 4 \mod 5$. Να δειχθεί ότι η εξίσωση $x^2 \equiv 5 \mod p$ έχει λύση.

Θέμα 2

(1) Να αποδειχτεί ότι για κάθε πρώτο p το πολυώνυμο $1 + x + \cdots + x^{p-1} \in \mathbb{Z}[x]$ είναι ανάγωγο.
(2) Υπάρχει σώμα με 10 στοιχεία; Να αποδειχθεί ότι σε ένα σώμα με 8 στοιχεία κάθε μη μηδενικό στοιχείο είναι πρωταρχικό.
(3) Να εξεταστεί αν οι δακτύλιοι $\mathbb{F}_{p^h}$ και $\mathbb{Z}/p^h\mathbb{Z}$ είναι ισόμορφοι.

Θέμα 3.

(1) Δείξτε ότι ο δακτύλιος $\mathbb{F} = \mathbb{F}_3[x]/(x^2 - x - 1)$ είναι σώμα.
(2) Είναι η ομάδα $\mathbb{F}^*$ κυκλική; Αν ναι υπολογίστε ένα γεννήτορά της.
(3) Δίνεται ένα ανάγωγο πολυώνυμο $f(x) \in \mathbb{F}_p[x]$. Να αποδειχθεί ότι αν α είναι μία ρίζα του, τότε και το α^p είναι επίσης μία ρίζα του.

Θέμα 4.

(1) Να περιγραφεί το σύστημα κρυπτογράφησης RSA.
(2) Να παραγοντοποιηθεί με την μέθοδο Fermat ο αριθμός 70747.
(3) Να αποδειχθεί ότι στο σώμα των ρητών για p πρώτο, το p^2-κυκλοτομικό πολυώνυμο $\Phi_{p^2}(x)$ δίνεται από τον τύπο:

$$\Phi_{p^2}(x) = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1.$$

Διάρκεια εξέτασης 2 ώρες 45 λεπτά