# Χαν Πεπερασμένα Σώματα και Κρυπτογραφία

## Κεφάλαιο 1 Στοιχειώδης Θ. Αριθμών

Γνώση των τεχνικών: Αλγόριθμος Ευκλείδη, εύρεση μεγίστου κοινού διαιρέτη, επίλυσης συστήματος ισοδυναμιών (Κινέζικο θεώρημα), λύση της $ax \equiv b \bmod m$ και της $ax + by = c$.

Αριθμητικές συναρτήσεις και ιδιότητες τους, ο νόμος αντιστροφής του Möbius

## Κεφάλαιο 2 Θεωρία Δακτυλίων

Ορισμοί: Δακτυλίου, ιδεώδους ομομορφισμού.
Θεώρημα ισομορφισμών δακτυλίων (2.3.2) με απόδειξη.
Θεώρημα 2.4.3.
Ανάγωγα πολυώνυμα, κριτήρια αναγωγιμότητας
Χρήση του θεωρήματος Eisenstein.

Χαρακτηριστική δακτυλίου και σώματος. Η χαρακτηριστική σώματος είναι πρώτος αριθμός.

Πρώτα και μέγιστα ιδεώδη, Οι χαρακτηρισμοί τους από τα θεωρήματα 2.4.11, 2.4.12

## Κεφάλαιο 3 Νόμος τετραγωνικής αντιστροφής

Υπολογισμός συμβόλων Legendre. SOS: Για ποιους πρώτους $p$ η ισοτιμία $x^2 \equiv 5 \bmod p$ έχει λύση και παρόμοια προβλήματα.

## Κεφάλαιο 4 Πεπερασμένα Σώματα

Ορισμοί (σώμα διάσπασης επέκτασης).

4.2.1 (με απόδειξη) 4.3.2 (SOS ή απόδειξη)

Τάξη στοιχείων πεπερασμένου σώματος.
Κριτήρια πολ/κων ριζών

Θεώρημα 4.3.6 (χωρίς απόδειξη). Εύρεση πρωταρχικού στοιχείου.

Προτάσεις 4.3.12, 4.3.13, 4.3.14, 4.3.15 SOS και οι αποδείξεις

Θεωρήματα 4.4.4, 4.4.5 SOS και οι αποδείξεις

Θεώρημα 4.5.4 SOS

Αλγόριθμος εύρεσης πρωταρχικής ρίζας.

Θεώρημα 4.6.1 SOS.

Απόδειξη και χρήση του τύπου μέτρησης αναγώγων πολυωνύμων.

Κυκλοτομικά πολυώνυμα Ορισμός.

Χρήση αναδρομικών τύπων για την εύρεση τους

Κεφάλαιο 5 Απλά Κρυπτοσυστήματα

Γνώση των κρυπτοσυστημάτων

Κεφάλαιο 6 Κρυπτοσυστήματα Ανοιχτού Κλειδιού.

Το σύστημα RSA, περιγραφή και κατανόηση του αλγόριθμος.

Αλγόριθμος υψωσης σε δύναμη (SOS)

El Gamal, περιγραφή και κατανόηση.

Το πρόβλημα του διακριτού λογαρίθμου.

## Κεφάλαιο 7 Ελλειπτικές Καμπύλες.

Ορισμός προβολικού επιπέδου

Λίστα του προβλήματος των Πυθαγορείων τριάδων

Ορισμός ελλ. καμπύλης, τύποι πρόσθεσης

Ελλειπτικά κρυπτοσυστήματα: ElGamal σε ελλειπτικές καμπύλες

## Κεφάλαιο 8 Μέθοδοι Παραγοντοποίησης

Πρόταση 8.1.1, Ορισμοί ψευδοπρώτων και πρώτων Carmichael

Αλγόριθμος παραγοντοποίησης του Fermat (SOS και η χρήσιμότητα)