## Ύλη εξετάσεων ψηφίων Α. Κοντογεώργη 2015

Οι σελίδες και η αρίθμηση των παραγράφων αφορούν την τελευταία έκδοση η οποία είναι διαθέσιμη στον σύνδεσμο:

http://eclass.uoa.gr/modules/document/file.php/MATH443/NumberTheoryNov.pdf

Η θεωρία των αριθμητικών συναρτήσεων αναπτύσεται στην παράγραφο 1.6 σελίδες 13-18 του βιβλίου μας Πεπερασμένα σώματα και κρυπτογραφία το οποίο βρίσκεται διαθέσιμο στον σύνδεσμο:

http://eclass.uoa.gr/modules/document/file.php/MATH443/FiniteFieldsCrypto.pdf

1. Διαιρετότητα και πρώτοι αριθμοί 1.1, σελ. 3.
2. Διαιρετότητα 1.2, σελ. 8
3. Πρώτοι αριθμοί 1.3, σελ. 13. Η παράγραφος 1.3.1 σελ. 19 έως 29 είναι εκτός ύλης. Η πρόταση 1.3.21 στην σελίδα 26 είναι εντός.
4. Η παράγραφος 1.5 στην σελίδα 34 είναι εντός ύλης.
5. Η παράγραφος 1.6 στην σελίδα 43 είναι εντός ύλης. Θα πρέπει επίσης ο φοιτητής/ια να έχει ευχέρεια στον υπολογισμό ΜΚΔ και ΕΚΠ με τον αλγόριθμο του Ευκλείδη.
6. Η παράγραφος 1.7 στην σελίδα 47 είναι εντός ύλης.
7. Γραμμικές Διοφαντικές εξισώσεις 2.2, σελ. 56, μόνο η περίπτωση των δύο μεταβλητών, δηλαδή η παράγραφος 2.2.1 είναι εκτός.
8. Πυθαγόρειες τριάδες εντός ύλης, παρ. 2.3 σελ. 61. Η εικασία του Fermat σελ. 63 μέχρι και σελίδα 70 είναι εκτός ύλης.
9. Οι παράγραφοι 3.1 σελ. 75, 3.2 σελ. 78, 3.2.1 σελ. 81 είναι εντός ύλης. Η παράγραφος 3.2.2 σελ. 83, 3.2.3, 85 είναι εκτός ύλης.
10. Το κριτήριο παραγοντοποίησης του Fermat 3.4.1 σελ. 89 είναι εντός ύλης.

11. Το κεφάλαιο των ισοδυναμιών είναι όλο εντός ύλης εκτός από τον υπολογισμό του Πάσχα 4.4.4 σελ. 118 και τον αλγόριθμο ύψωση σε δύναμη παρ. 4.5 σελ. 118. Η παράγραφος της κρυπτογραφίας 4.6, σελ. 120 είναι εκτός ύλης μέχρι την σελ. 126.

12. Η επίλυση ισοδυναμιών ανωτέρου βαθμού είναι εντός ύλης παρ. 4.7 σελ. 126. Η παράγραφοι 4.8 σελ. 136 και 4.9 142 είναι εκτός ύλης.

13. Από το κεφάλαιο 5 Τετραγωνικά υπόλοιπα, το σύμβολο του Legendre ο τετραγωνικός νόμος αντιστροφής, το σύμβολο του Jacobi. Εκτός ύλης ο αλγόριθμος του Eisenstein 5.2.15 καθώς και η παράγραφοι 5.2.3 σελ. 172 και 5.3 σελ. 179.

14. Η παράγραφος 5.4 σελ. 184 εντός ύλης όπως και η 5.4.2 σελ. 200. Από την παράγραφο 5.4.3 205 μέχρι το τέλος του βιβλίου εκτός ύλης.

**Δεξιότητες**

Οι φοιτητές/τριες θα πρέπει να μπορούν να λύνουν προβλήματα:

1. Υπολογισμού μέγιστου κοινού διαιρέτη

2. Επίλυση γραμμικών Διοφαντικών εξισώσεων με 2 αγνώστους (και το πρόβλημα των θετικών λύσεων)

3. Επίλυση συστημάτων με την μέθοδο του Κινέζου

4. Να ελέγχουν αν ένας ακέραιος είναι τετραγωνικό υπόλοιπο modulo $p$ και επίσης να γνωρίζουν να υπολογίζουν για ποια $p$ είναι ένας ακέραιος τετραγωνικό υπόλοιπο.

5. Θα πρέπει να γνωρίζουν να λύνουν εξισώσεις $f(x) \equiv 0 \mathrm{mod} p^k$ με την μέθοδο της αναγωγής στην εξίσωση $f(x) \equiv 0 \mathrm{mod} p^{k-1}$.

6. Θα πρέπει να γνωρίζουν να υπολογίζουν σύμβολα του Legendre και να μπορούν να απαντήσουν αν μια εξίσωση της μορφής $x^2 \equiv a \mathrm{mod} p$, έχει λύση για $p$ πρώτο.

7. Θα πρέπει να μπορούν να υπολογίζουν μια πρωταρχική ρίζα $\mathrm{mod} m$, όταν αυτή υπάρχει για σχετικά μικρό $m$.