ΚΑΤΑΛΟΓΟΣ ΜΑΘΗΜΑΤΩΝ/ΥΛΗ/ΒΙΒΛΙΟΓΡΑΦΙΑ

Μάθημα: ΑΛΓΕΒΡΑ

Εξεταστέα ύλη:

1. Ομάδες, υποομάδες. Ειδικές κατηγορίες ομάδων: Ομάδες μεταθέσεων, τροχιές κύκλοι, εναλλάσσουσες ομάδες. Κυκλικές ομάδες, υποομάδες σύμπλοκα, Ομάδες πηλίκα, το θεώρημα Lagrange. Ευθέα γινόμενα ομάδων.
2. Γεννήτορες μιας ομάδας, η δομή των πεπερασμένα παραγώμενων αβελιανων ομάδων. Ομάδες με τάξη μικρότερη ή ίση του 8.
3. Ομομορφισμοι, ισομορφισμοί ομάδων, θεωρήματα ισομορφισμών. Δράσεις ομάδων σε σύνολα, τροχιές, τα θεωρήματα του Sylow, p-ομάδες, Η εξίσωση κλάσεων.
4. Δακτύλιοι και σώματα. Ακέραιες περιοχές, χαρακτηριστική δακτυλίου, σώμα πηλίκου.
5. Δακτύλιοι πολυωνύμων, διαίρεση, ανάγωγα πολυώνυμα.
6. Ομομορφισμοί και δακτύλιοι πηλίκα. Πρώτα και μέγιστα ιδεώδη, η δομή των ιδεωδών σε πολυωνυμικό δακτύλιο με συντελεστές από ένα σώμα.
7. Περιοχές μονοσήμαντης ανάλυσης, Ευκλείδειες περιοχές. Ομάδα των μονάδων.
8. Επεκτάσεις σωμάτων, αλγεβρικά και υπερβατικά στοιχεία, βαθμός επέκτασης. Πεπερασμένα σώματα.
9. Modules, άλγεβρες, τάξη module, το θεώρημα δομής modules πάνω από περιοχές κυριών ιδεωδών.

Βιβλιογραφία: J.B. Fraleigh, Εισαγωγή στην Άλγεβρα. Πανεπιστημιακές Εκδόσεις Κρήτης.

Μάθημα: ΑΝΑΛΥΣΗ

Εξεταστέα ύλη

1. Στοιχεία Μετρικών Χώρων
2. Ακολουθίες και Σειρές
3. Συνέχεια
4. Διαφόριση
5. Ολοκλήρωση Riemann
6. Ακολουθίες και Σειρές Συναρτήσεων
7. Συναρτήσεις Πολλών Μεταβλητών

Βιβλιογραφία: Πραγματική Ανάλυση. Μ. Ανούσης, Α. Τσολομύτης, Β. Φελουζής (όλο το βιβλίο)

Μάθημα: ΑΡΙΘΜΗΤΙΚΗ ΑΝΑΛΥΣΗ

Εξεταστέα ύλη:

1. Αριθμητική επίλυση μη-γραμμικών αλγεβρικών εξισώσεων και συστημάτων εξισώσεων
Επίλυση μη-γραμμικών εξισώσεων. Η μέθοδος της διχοτόμησης. Το θεώρημα σταθερού σημείου του Banach. Επαναληπτικές μέθοδοι (1) γενική μέθοδος, (2) Newton-Raphson, (3) εφαπτομένης. Αριθμητική επίλυση συστημάτων αλγεβρικών εξισώσεων με την μέθοδο Newton-Raphson.
2. Αριθμητική επίλυση γραμμικών συστημάτων
Η μέθοδος απαλοιφής του Gauss και η ανάλυση LU. Ανάλυση Cholesky για συμμετρικούς και θετικά ορισμένους πίνακες. Κατάσταση γραμμικών συστημάτων. Νόρμες διανυσμάτων και πινάκων. Δείκτης κατάστασης πίνακα. Ευστάθεια γραμμικών συστημάτων. Αριθμητική επίλυση γραμμικών συστημάτων με τις επαναληπτικές μεθόδους Jacobi και Gauss-Seidel.
3. Πολυωνυμική παρεμβολή
Παρεμβολή Lagrange και Newton. Πολυώνυμα Chebyshev. Παρεμβολή Hermite. Παρεμβολή με splines, με τμηματικά γραμμικές συναρτήσεις και κυβικές splines.
4. Αριθμητική ολοκλήρωση
Τύποι ολοκλήρωσης των Newton-Cotes. Μέθοδοι (α) ορθογωνίου (β) τραπεζίου (γ) Simpson. Τύποι ολοκλήρωσης του Gauss.
5. Ελάχιστα τετράγωνα
Βέλτιστη διακριτή προσέγγιση. Βέλτιστη συνεχής προσέγγιση. Προσέγγιση με πολυώνυμα.
6. Αριθμητική επίλυση συνήθων διαφορικών εξισώσεων (προβλήματα αρχικών τιμών)
Οι έννοιες της σύγκλισης, ευστάθειας και συνέπειας για τις μεθόδους αριθμητικής επίλυσης προβλημάτων αρχικών τιμών. Θεωρητική μελέτη των γενικών s-βηματικών γραμμικών μεθόδων. Οι μέθοδοι: (1) αναλυτής και μη-αναλυτής Euler, (2) τραπεζίου, (3) μέσου σημείου (4) Adams-Bashforth, Adams-Moulton και πρόβλεψης-διόρθωσης και (5) Runge-Kutta.
7. Αριθμητική επίλυση συνήθων διαφορικών εξισώσεων (προβλήματα συνοριακών τιμών)
Η μέθοδος της βολής και η μέθοδος των πεπερασμένων διαφορών.

Προτεινόμενα συγγράμματα:

- Εισαγωγή στην αριθμητική ανάλυση, Γ.Δ. Ακριβής & Β.Α. Δούγαλης, Πανεπιστημιακές Εκδόσεις Κρήτης, 4η έκδοση (2002).
- Αριθμητικές μέθοδοι και προγράμματα για μαθηματικούς υπολογισμούς, G.E. Forsythe, M.A. Malcolm & C.B. Moler, μετάφραση από τους Γ.Δ. Ακριβή & Β.Α. Δούγαλη, Πανεπιστημιακές Εκδόσεις Κρήτης, (1997).
- Αριθμητική Ανάλυση, Γ.Σ. Σοφιανός & Ε.Θ. Τυχόπουλος, Εκδόσεις ΑΘ. Σταμούλης, Αθήνα 2005.

Μάθημα: <u>ΓΡΑΜΜΙΚΗ ΑΛΓΕΒΡΑ</u>

Εξεταστέα ύλη:

Ορισμοί γραμμικού χώρου. Γραμμικές απεικονίσεις.
Πίνακες, πράξεις πινάκων, πίνακες και γραμμικές απεικονίσεις Τάξη πίνακα, όμοιοι πίνακες.
Λύση γραμμικών συστημάτων. Ορίζουσες, υπολογισμός, εφαρμογές στους πίνακες και στην λύση γραμμικών συστημάτων.
Αναλλοίωτοι υπόχωροι, ιδιοτιμές ιδιοδιανύσματα.
Θεώρημα των Caley-Hamilton, ελάχιστο και χαρακτηριστικό πολυώνυμο.
Διαγώνοποιήσιμοι, Τριγωνοποιήσιμοι. Κανονική μορφή Jordan.
Γραμμικές μορφές, Δυικός χώρος. Διγραμμικές μορφές, τετραγωνικές μορφές Εσωτερικά γινόμενα. Ερμιτιανές και συμμετρικές απεικονίσεις. Ισομετρίες ορθογώνιες απεικονίσεις.

Βιβλιογραφία: Σ. Ανδρεαδάκης, Γραμμική Άλγεβρα. Εκδόσεις Συμμετρία.

<u>Μάθημα: ΔΙΑΦΟΡΙΚΕΣ ΕΞΙΣΩΣΕΙΣ</u>

Εξεταστέα ύλη:

1. Διαφορικές εξισώσεις 1ης τάξης ([BD]: Κεφάλαιο 2)
2. Διαφορικές εξισώσεις 2ης τάξης ([BD]: Κεφάλαιο 3)
3. Γραμμικές διαφορικές εξισώσεις ανώτερης τάξης ([BD]: Κεφάλαιο 4)
4. Επίλυση γραμμικών διαφορικών εξισώσεων 2ης τάξης με τη μέθοδο των δυναμοσειρών ([BD]: Κεφάλαιο 5)
5. Συστήματα γραμμικών διαφορικών εξισώσεων 1ης τάξης ([BD]: Κεφάλαιο 6)
6. Μη γραμμικές διαφορικές εξισώσεις και ευστάθεια ([BD]: Κεφάλαιο 9. Ενότητες 9.1-9.6)
7. Εισαγωγή στις μερικές διαφορικές εξισώσεις ([ΝΣ]: Κεφάλαιο 1)
8. Εξισώσεις ελλειπτικού τύπου ([ΝΣ]: Κεφάλαιο 2)
9. Εξισώσεις παραβολικού τύπου ([ΝΣ]: Κεφάλαιο 3)
10. Εξισώσεις υπερβολικού τύπου ([ΝΣ]: Κεφάλαιο 4. Ενότητες 4.1-4.4)
11. 2 και 3 χωρικές διαστάσεις ([ΝΣ]: Κεφάλαιο 5)
12. Μη φραγμένα πεδία ([ΝΣ]: Κεφάλαιο 6. Ενότητες 6.1, 6.2, 6.4)

Ενδεικτική Βιβλιογραφία:

[BD] William E. Boyce - Richard C. DiPrima «Στοιχειώδεις διαφορικές εξισώσεις και προβλήματα συνοριακών τιμών» Πανεπιστημιακές Εκδόσεις ΕΜΠ, (1999)
[ΝΣ] Νικόλαος Μ. Σταυρακάκης «Εξισώσεις Μερικών Παραγώγων για τις επιστήμες και την τεχνολογία» Αθήνα, Ιανουάριος 2002.

<u>Μάθημα: ΔΙΑΦΟΡΙΚΗ ΓΕΩΜΕΤΡΙΑ</u>

Εξεταστέα ύλη:

Διαφορίσιμες καμπύλες στο χώρο. Παραμέτρηση με μήκος τόξου. Η καμπυλότητα και η στρέψη κανονικής καμπύλης. Το τρίεδρο του Frenet. Το θεμελιώδες θεώρημα της τοπικής θεωρίας καμπύλων. Κανονικές επιφάνειες στο χώρο. Συστήματα συντεταγμένων και ειδικές μορφές παραμετρήσεων. Αλλαγή συντεταγμένων. Διαφορίσιμες απεικονίσεις. Το εφαπτόμενο επίπεδο και η έννοια του διαφορικού μιας απεικόνισης. Η πρώτη θεμελιώδης μορφή. Προσανατολισμός. Απεικόνιση του Gauss και ο τελεστής σχήματος. Η δεύτερη θεμελιώδης μορφή. Καμπυλότητα Gauss και η μέση καμπυλότητα. Ισομετρίες. Τα σύμβολα Christoffel και το θεώρημα Ergegium του Gauss. Η έννοια της εσωτερικής γεωμετρίας. Γεωδαισιακές γραμμές μιας επιφάνειας.

ΒΙΒΛΙΟΓΡΑΦΙΑ:

1. Στοιχειώδης διαφορική γεωμετρία, O'neil Barrett, Ίδρυμα Τεχνολογίας & Έρευνας-Πανεπιστημιακές Εκδόσεις Κρήτης, (2002)
2. Διαφορική Γεωμετρία, Ν.Κ.Στεφανίδης, Σ. Γιαχούδης & ΣΙΑ Ο.Ε., (2014).
3. Στοιχειώδης Διαφορική Γεωμετρία, Κουτρουφιώτης Δημήτρης, LIBERAL BOOKS Μονοπρόσωπη ΕΠΕ, (2006).
4. Στοιχειώδης διαφορική γεωμετρία, Pressley Andrew, , Ίδρυμα Τεχνολογίας &Έρευνας-Πανεπιστημιακές Εκδόσεις Κρήτης, (2011).

Μάθημα<u>: ΔΙΔΑΚΤΙΚΗ ΜΑΘΗΜΑΤΙΚΩΝ</u>

Εξεταστέα ύλη:

Στοιχεία ψυχολογίας της μάθησης των Μαθηματικών και διδακτικές αρχές. (J. Piaget. J. S. Bruner)
Θεωρία μάθησης R. M. Gagné. Η γενετική άρχή του E. Wittmann. Θεωρία Κονστρουκτιβισμού.
Μοντέλα Διδασκαλίας Μαθηματικών. Διδακτικό μοντέλο του R. Glaser.
Διαδικασία Επίλυσης Προβλήματος (Problem Solving).
Μαθηματικά και Εκπαίδευση. Σχέση ιστορίας και διδασκαλίας Μαθηματικών. Σκοποί μαθηματικής εκπαίδευσης.
Φιλοσοφία Μαθηματικών. Πλατωνισμός. Φορμαλισμός. Ενορατισμός. Ημιεμπειρισμός του I. Lakatos.
Διδασκαλία Άλγεβρας. Διδασκαλία αρνητικών αριθμών. Διδασκαλία Γεωμετρίας. Διδασκαλία Ανάλυσης.
Ειδικά θέματα διδακτικής Μαθηματικών. Διδασκαλία της απόδειξης. Το λάθος στην διαδικασία μάθησης. Δυσλεξία και Μαθηματικά.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Χαράλαμπος Τουμάσης: Διδακτική Μαθηματικών. Εκδόσεις Gutenberg. (Τυπωθήτω-Δαρδανός)

Μάθημα: <u>ΔΙΑΚΡΙΤΑ ΜΑΘΗΜΑΤΙΚΑ</u>
Εξεταστέα ύλη:
1. ΣΥΝΟΛΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ
Συνδυασμοί συνόλων. Πεπερασμένα και άπειρα σύνολα. Μη αριθμήσιμα απειροσύνολα. Η μαθηματική επαγωγή. Αρχή του εγκλεισμού και του αποκλεισμού. Προτάσεις.
2. ΥΠΟΛΟΓΙΣΙΜΟΤΗΤΑ ΚΑΙ ΤΥΠΙΚΕΣ ΓΛΩΣΣΕΣ
Το παράδοξο του Rusell και μη υπολογισιμότητα. Διατεταγμένα σύνολα. Γλώσσες. Γραμματικές δομής φράσεως. Τύποι γραμματικών και γλωσσών.
3. ΜΕΤΑΘΕΣΕΙΣ, ΣΥΝΔΥΑΣΜΟΙ ΚΑΙ ΔΙΑΚΡΙΤΗ ΠΙΘΑΝΟΤΗΤΑ
Οι κανόνες του αθροίσματος και του γινομένου. Μεταθέσεις. Συνδυασμοί. Δημιουργία μεταθέσεων και συνδυασμών. Διακριτή πιθανότητα. Δεσμευμένη πιθανότητα.
4. ΣΧΕΣΕΙΣ ΚΑΙ ΣΥΝΑΡΤΗΣΕΙΣ
Ένα σχεσιακό πρότυπο για βάσεις δεδομένων. Ιδιότητες των διμελών σχέσεων. Σχέσεις ισοδυναμίας και διαμερίσεις. Σχέσεις και δικτυωτά μερικής διάταξης. Αλυσίδες και αντιαλυσίδες. Συναρτήσεις και η αρχή του περιστερώνα.
5. ΓΡΑΦΗΜΑΤΑ ΚΑΙ ΕΠΙΠΕΔΑ ΓΡΑΦΗΜΑΤΑ
Βασική ορολογία. Πολυγραφήματα και βεβαρημένα γραφήματα. Μονοπάτια και κυκλώματα. Ελάχιστα μονοπάτια σε βεβαρημένα γραφήματα. Μονοπάτια και κυκλώματα Euler. Μονοπάτια και κυκλώματα Hamilton. Το πρόβλημα του περιοδεύοντος πωλητή. Παράγοντες γραφήματος. Επίπεδα γραφήματα.
6. ΔΕΝΔΡΑ ΚΑΙ ΣΥΝΟΛΑ ΤΟΜΗΣ
Δένδρα. Δένδρα με ρίζες. Μήκη μονοπατιών σε δένδρα με ρίζα. Κώδικες προθέματος. Δυαδικά δένδρα αναζήτησης.
7. ΜΗΧΑΝΕΣ ΠΕΠΕΡΑΣΜΕΝΩΝ ΚΑΤΑΣΤΑΣΕΩΝ
Μηχανές πεπερασμένων καταστάσεων. Μηχανές πεπερασμένων καταστάσεων ως μοντέλα φυσικών συστημάτων. Ισοδύναμες μηχανές. Μηχανές πεπερασμένων καταστάσεων ως αναγνωριστές γλώσσας.
8. ΑΝΑΛΥΣΗ ΑΛΓΟΡΙΘΜΩΝ
Χρονική πολυπλοκότητα των αλγορίθμων. Ένας αλγόριθμος για την εύρεση ενός ελαχίστου μονοπατιού. Πολυπλοκότητα των προβλημάτων. Πρακτικώς επιλύσιμα και δυσεπίλυτα προβλήματα
9. ΔΙΑΚΡΙΤΕΣ ΑΡΙΘΜΗΤΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΙ ΓΕΝΝΗΤΡΙΕΣ ΣΥΝΑΡΤΗΣΕΙΣ
Χειρισμός αριθμητικών συναρτήσεων. Η ασυμπτωτική συμπεριφορά των αριθμητικών συναρτήσεων. Γεννήτριες συναρτήσεις. Συνδυαστικά προβλήματα.
10. ΑΝΑΔΡΟΜΙΚΕΣ ΣΧΕΣΕΙΣ ΚΑΙ ΑΝΑΔΡΟΜΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ
Αναδρομικές σχέσεις. Γραμμικές αναδρομικές σχέσεις με σταθερούς συντελεστές. Ομογενείς λύσεις. Ειδικές λύσεις. Ολικές λύσεις. Λύση με τη μέθοδο των γεννητριών συναρτήσεων. Αλγόριθμοι ταξινόμησης. Αλγόριθμοι πολλαπλασιασμού πινάκων.

Βιβλίο: C. L. Liu, Στοιχεία Διακριτών Μαθηματικών, Πανεπιστημιακές Εκδόσεις Κρήτης, 2006.

<u>Μάθημα: ΘΕΩΡΙΑ ΣΥΝΟΛΩΝ</u>
Εξεταστέα ύλη:
Κεφ. 1: Εισαγωγή στα σύνολα.
Κεφ. 2: Σχέσεις, Συναρτήσεις, και Διατάξεις.
Κεφ. 3: Το σύνολο των φυσικών αριθμών.
Κεφ. 4: Πεπερασμένα και αριθμήσιμα σύνολα.
Κεφ. 5: Το σύνολο των πραγματικών αριθμών.
Κεφ. 6: Πληθάριθμοι.
Κεφ. 7: Διατακτικοί αριθμοί.
Κεφ. 8: Άλεφς.
Κεφ. 10: Η αριθμητική των πληθαρίθμων.

Προτεινόμενο σύγγραμμα: Karel Hrbacek and Thomas Jech, Introduction to Set Theory, Marcel-Dekker, Inc. New York,1984.

Μάθημα: <u>ΙΣΤΟΡΙΑ ΜΑΘΗΜΑΤΙΚΩΝ</u>
Εξεταστέα ύλη:
Πρώιμα αριθμητικά συστήματα. Αιγυπτιακά και Βαβυλωνιακά Μαθηματικά.
Απαρχές των Ελληνικών Μαθηματικών. Ο χρυσός αιώνας.Η εποχή του Πλάτωνα.Αλεξανδρινή Εποχή. Παρακμή των Ελληνικών Μαθηματικών. Αλεξανδρινή Σχολή: Ευκλείδης, Ερατοσθένης, Αρχιμήδης
Διόφαντος, Fibonacci. Cardano, Fermat. Descartes και Newton.
Η ανάπτυξη της θεωρίας πιθανοτήτων: Pascal, Bernoulli, Laplace
Θεωρία Αριθμών: Από τον Fermat στον Euler, Gauss.
19ος αιώνας της Γεωμετρίας: Gauss, Bolyai, Lobatschefskij, Monge, Steiner, Felix Klein.
19ος αιώνας της Ανάλυσης: Weierstrass, Cantor, Dedekind
Άλγεβρα: Boole, De Morgan, 20ου αιώνα Hamilton, Grassmann, Cayley
Απαρχές 20ου αιώνα: Poincare, Hilbert

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Van der Waerden. Η αφύπνιση της Επιστήμης. Πανεπιστημιακές Εκδόσεις Κρήτης.
2. Cral Boyer-Uta Merzbach. Η Ιστορία των Μαθηματικών. Εκδόσεις Γ.Α. Πνευματικού.

Μάθημα: <u>ΜΕΘΟΔΟΛΟΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΄ΕΡΕΥΝΑΣ</u>

Εξεταστέα ύλη:

Η Διαδικασία Διεξαγωγής Έρευνας: Χρησιμοποιώντας Ποσοτικές και Ποιοτικές Προσεγγίσεις
Αναγνώριση ενός Ερευνητικού Προβλήματος
Ανασκόπηση της Βιβλιογραφίας
Προσδιορισμός Σκοπού και Ερευνητικών Ερωτημάτων ή Υποθέσεων
Συγκέντρωση Ποσοτικών Δεδομένων
Ανάλυση και Ερμηνεία Ποσοτικών Δεδομένων
Συγκέντρωση Ποιοτικών Δεδομένων
Ανάλυση και Ερμηνεία Ποιοτικών Δεδομένων
Ποιοτικές μέθοδοι
Μικτές μέθοδοι και διαδικασίες

Βιβλιογραφία:

1. John W. Creswell Research Design Qualitative, Quantitative, And Mixed Methods Approaches, SAGE Publications, 2009.
2. Louis Cohen, Lawrence Manion and Keith Morrison, Research Methods in Education. Sixth Edition, Routledge, 2011.
3. Barry H. Cohen and R. Brooke Lea, Essentials of Statistics for the Social and Behavioral Sciences, Wiley, 2004.

<u>Μάθημα: ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΣΤΗΝ ΕΚΠΑΙΔΕΥΣΗ</u>

Εξεταστέα ύλη:

Βασικές Έννοιες και Ορισμοί
Συμπεριφορισμός
Γνωσιακές Θεωρίες
Διδακτική σχεδίαση
Εποικοδομισμός
Κοινωνικός Εποικοδομισμός
Κονεκτιβισμός
Κονστραξιονισμός
Παιχνιδοκεντρική Μάθηση

Βιβλιογραφία:

1. Σταύρος Δημητριάδης, Θεωρίες Μάθησης και Εκπαιδευτικό Λογισμικό, Κάλλιπος, 2015.
2. Christian Depover, Thierry Karsenti, Βασίλης Κόμης, Διδασκαλία με τη χρήση της τεχνολογίας, Κλειδάριθμος 2010.

<u>Μάθημα: ΠΙΘΑΝΟΤΗΤΕΣ</u>

Εξεταστέα ύλη:

1. Αξιωματική Θεμελίωση Πιθανοτήτων. Χώρος πιθανότητας.
2. Πείραμα τύχης. Ενδεχόμενα. Βασικοί κανόνες πιθανοτήτων.
2. Συνδυαστική ανάλυση. Διατάξεις, Μεταθέσεις, Συνδυασμοί.
3. Διακριτές τυχαίες μεταβλητές.
4. Μέση τιμή και διακύμανση διακριτών τυχαίων μεταβλητών.
5. Συνεχείς τυχαίες μεταβλητές.
6. Οι κυριότερες διακριτές και συνεχείς κατανομές πιθανοτήτων (Bernoulli, Διωνυμική, Poisson, Γεωμετρική, Υπεργεωμετρική, Κανονική, Συνεχής Ομοιόμορφη, Εκθετική).
7. Πολυδιάστατες κατανομές. Περιθωριακές και υπό-συνθήκη κατανομές. Ανεξαρτησία. Συνδιακύμανση και Συντελεστής συσχέτισης. Επαναλαμβανόμενη μέση τιμή και διασπορά, υπό-συνθήκη μέση τιμή και διασπορά.
8. Ακολουθίες τυχαίων μεταβλητών και είδη σύγκλισης.
9. Κεντρικό Οριακό Θεώρημα και Ισχυρός Νόμος των Μεγάλων Αριθμών.
10. Ροπογεννήτριες συναρτήσεις.

Ενδεικτική Βιβλιογραφία:

- Κούτρας Μ., Εισαγωγή στις Πιθανότητες, Θεωρία και Εφαρμογές, Εκδόσεις Σταμούλη, 2012.
- Ross S, (μετάφραση Φελουζής Ε), Βασικές Αρχές Θεωρίας Πιθανοτήτων, Κλειδάριθμος 2012.
- P. Hoel, S. Port, και C. Stone, Εισαγωγή στη θεωρία πιθανοτήτων. Πανεπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο, 2002.
- Κουνιάς Σ και Μωυσιάδης Χ, Θεωρία Πιθανοτήτων Ι, Εκδόσεις Ζήτη 1999.
- Ξένου Θ.Π., Πιθανότητες, Εκδόσεις Ζήτη, 2012.

Μάθημα: ΠΛΗΡΟΦΟΡΙΚΗ

Εξεταστέα ύλη:
Κεφάλαιο 2. Τύποι, τελεστές και παραστάσεις
Μεταβλητές. Τύποι δεδομένων και μεγέθη. Σταθερές. Δηλώσεις. Αριθμητικοί Τελεστές. Συσχετιστικοί και λογικοί τελεστές. Μετατροπές τύπων. Τελεστές αύξησης και μείωσης. Τελεστές Πράξεων με bit. Τελεστές αντικατάστασης και παραστάσεις. Παραστάσεις υπό συνθήκη. Προτεραιότητα και σειρά υπολογισμών.
Κεφάλαιο 3. Η ροή του ελέγχου
Εντολές και μπλοκ. if-else. else-if. switch. Βρόχοι – while και for. Βρόχοι –do-while. break και continue. goto και ετικέτες.
Κεφάλαιο 4. Συναρτήσεις και δομή του προγράμματος
Τα βασικά στοιχεία των συναρτήσεων. Συναρτήσεις που επιστρέφουν μη ακέραιες τιμές. Εξωτερικές μεταβλητές. Κανόνες εμβέλειας. Αρχεία-επικεφαλίδες. Στατικές μεταβλητές. Μεταβλητές register. Δόμηση σε μπλοκ. Απόδοση αρχικών τιμών. Αναδρομικότητα. Ο προ-επεξεργαστής της C.
Κεφάλαιο 5. Δείκτες και πίνακες
Δείκτες και διευθύνσεις. Δείκτες και ορίσματα συναρτήσεων. Δείκτες και πίνακες. Αριθμητική διευθύνσεων. Δείκτες χαρακτήρα και συναρτήσεις. Πίνακες δεικτών και δείκτες που δείχνουν δείκτες. Πολυδιάστατοι πίνακες. Απόδοση αρχικής τιμής σε πίνακες δεικτών. Δείκτες και πολυδιάστατοι πίνακες. Ορίσματα γραμμής διαταγών. Δείκτες σε συναρτήσεις. Περίπλοκες δηλώσεις.
Κεφάλαιο 6. Δομές
Τα βασικά για τις δομές. Δομές και συναρτήσεις. Πίνακες δομών. Δείκτες σε δομές. Αυτό-αναφορικές δομές. Αναζήτηση σε πίνακα. typedef. Ενώσεις. Πεδία bit.
Κεφάλαιο 7. Είσοδος και έξοδος
Πρότυπη είσοδος και έξοδος. Φορμαρισμένη έξοδος – printf. Λίστα μεταβαλλόμενου πλήθους ορισμάτων. Φορμαρισμένη είσοδος –scanf. Προσπέλαση αρχείων. Χειρισμός λαθών –stderr και exit. Είσοδος και έξοδος γραμμών. Διάφορες συναρτήσεις.

Βιβλίο: Brian Kernighan και Dennis M. Ritche, Η γλώσσα Προγραμματισμού C, Κλειδάριθμος, 1990.

Μάθημα: ΣΤΟΧΑΣΤΙΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ (Η ΣΤΟΧΑΣΤΙΚΕΣ ΑΝΕΛΙΞΕΙΣ)
Εξεταστέα ύλη:
1. Εισαγωγή στις βασικές έννοιες των στοχαστικών διαδικασιών.
2. Διαδικασίες Markov σε διακριτό χρόνο. Εξισώσεις Chapman – Kolmogorov.
3. Ταξινόμηση καταστάσεων και στάσιμες κατανομές.
4. Διαδικασίες Markov σε συνεχή χρόνο.
5. Διαδικασίες Γεννήσεως–Θανάτου.
6. Διαδικασία Poisson και σύνθετη διαδικασία Poisson.
7. Θεωρία Ανανέωσης.
8. Διαδικασίες Martingales.
9. Κίνηση Brown και τυχαίοι περίπατοι.

Ενδεικτική βιβλιογραφία:

- Ross S, Stochastic Processes, John Wiley, 1996.
- Gallager R.G., Stochastic Processes, Theory for Applications, Cambridge University Press, 2013.
- Stirzaker D, Stochastic Processes and Models, Oxford University

Μάθημα: ΤΟΠΟΛΟΓΙΑ
Εξεταστέα ύλη:
Κεφ. 2: Τοπολογικοί χώροι και Συνεχείς συναρτήσεις (Ενότητες 2-1 ως και 2-11).
Κεφ. 3: Συνεκτικότητα και Συμπάγεια (Από 3-1 ως και 3-3. Από 3-5 ως και "Επιπλέον Ασκήσεις: Δίκτυα").
Κεφ. 4: Αξιώματα αριθμησιμότητας και Διαχωριστικά αξιώματα (Από 4-1 ως και 4-4).
Κεφ. 5: Το Θεώρημα του Tychonoff (Από 5-1 ως και 5-3).
Κεφ. 6: Θεωρήματα Μετρικοποιησιμότητας και Παρασυμπάγεια.
Κεφ. 7: Πλήρεις μετρικοί χώροι, Χώροι του Baire (Ενότητες 7-1, 7-3, 7-7).

Προτεινόμενο σύγγραμμα: James R. Munkres, Topology. A first course, Prentice Hall, New Jersey, 1975.

Μάθημα: Μέθοδοι Εφαρμοσμένων Μαθηματικών
Εξεταστέα ύλη:
Βασικά στοιχεία ασυμπτωτικής ανάλυσης. Ασυμπτωτικές σειρές και σειρές Taylor. Η επαναληπτική μέθοδος επίλυσης αλγεβρικών εξισώσεων. Η μέθοδος *κανονικών διαταραχών* επίλυσης αλγεβρικών και διαφορικών εξισώσεων. Η μέθοδος των *ιδιαζουσών διαταραχών*. Η μέθοδος *Poincare-Lindstedt*. Η προσέγγιση *WKB*. Η μέθοδος των πολλαπλών κλιμάκων. Θεωρία *συνοριακού στρώματος*. Ασυμπτωτικά αναπτύγματα ολοκληρωμάτων και το λήμμα του *Watson*. Τεχνικές επιτάχυνσης της σύγκλισης σειρών. Θεωρία και τεχνικές προβλημάτων ιδιοτιμών. Επίλυση γραμμικών διαφορικών εξισώσεων με την μέθοδο των σειρών γύρω από κανονικά και ιδιάζοντα σημεία (κανονικά και μη κανονικά ιδιάζοντα σημεία).

Προτεινόμενα συγγράμματα:

(1) E.J. Hinch, "*Perturbation methods"*, Cambridge University Press, 1991

(2) Γ. Δάσιος, "*Εισαγωγή στην Ασυμπτωτική Ανάλυση*", Εκδόσεις Τσότρας, Αθήνα, 2016

(3) C.M. Bender, S.A. Orszag, "*Advanced Mathematical Methods for Scientists and Engineers I, "Asymptotic Methods and Perturbation Theory*", 1st ed., Springer-Verlag, New York, 1999 .

Μάθημα: <u>Κρυπτογραφία</u>

Εξεταστέα ύλη:

Αλγόριθμοι και κρυπτογραφία. Εισαγωγή στη θεωρία πολυπλοκότητας, γρήγορα επιλύσιμα προβλήματα και η κλάση πολυπλοκότητας P, δύσκολα υπολογιστικά προβλήματα και η κλάση πολυπλοκότητας NP, NP-πλήρη προβλήματα (το πρόβλημα SAT), το ερώτημα εάν P≠NP.

Μοντέλα Αξιολόγησης Ασφάλειας. Σχεδίαση Ασφαλών Κρυπτογραφικών Συστημάτων. Ορισμός Κρυπτογράφησης και Κρυπτανάλυσης. Θεωρία Πληροφορίας: Πιθανότητες, Εντροπία, Αμοιβαία Πληροφορία.

Διαρροή Πληροφορίας από το κρυπτοκείμενο. Τέλεια Μυστικότητα. Περίσσεια Γλώσσας. Ασάφεια Κλειδιού. Υπολογισμός μέσου αριθμού ψευδοκλειδιών (spurious keys). Εύρεση μήκους κρυπτοκειμένου που μηδενίζει το πλήθος των ψευδοκλειδιών (unicity Distance). Κρυπταλγόριθμοι ροής και τμήματος.

Κρυπτογραφικές Πράξεις. Κρυπταλγόριθμος Αναδιάταξης. Κρυπταλγόριθμος Μετατόπισης και Κρυπταλγόριθμος του Καίσαρα. Κρυπταλγόριθμος Αντικατάστασης. Ασφάλεια Μονοαλφαβητικής Αντικατάστασης. Γραμμικός Κρυπταλγόριθμος. Κρυπτανάλυση Γραμμικού Κρυπταλγόριθμου.

Κρυπταλγόριθμος Vigenere. Κρυπτανάλυση Vigenere: Έλεγχος Kassiski και δείκτης σύμπτωσης. Κρυπτοσύστημα σημειωματαρίου μιας χρήσης. Κρυπτοσύστημα Vernam. Κρυπταλγόριθμος Hill. Κρυπτανάλυση Hill. Κρυπτογράφηση γινομένου.

Κρυπτογραφικά σχήματα διαμοιραζόμενου κλειδιού. Δίκτυα Αντικατάστασης Μετάθεσης (SPN). Σχεδίαση Κουτιών Αντικατάστασης (SBoxes). Αρχές διάχυσης (diffusion) και σύγχυσης (confusion). Κρυπταλγόριθμος τμήματος.

Δίκτυα Feistel. Ασφάλεια Δικτύων Feistel: Μεταθέσεις, Αντίπαλος, Μαντείο, Ψευδοτυχαίες Μεταθέσεις και Συναρτήσεις. Αναλυτική παρουσίαση της σχεδίασης και της λειτουργίας των κρυπταλγορίθμων DES (Data Encryption Standard) και AES (Advanced Encryption Standard).

Τρόποι διασύνδεσης κρυπταλγόριθμων τμήματος. Τριπλή Κρυπτογράφηση και η επίθεση meet-in-the-middle. Αλγόριθμοι Προγράμματος Κλειδιού. Γραμμική και Διαφορική Κρυπτανάλυση.

Σχήματα κρυπτογράφησης δημόσιου κλειδιού. Η ιδέα των Diffie-Hellman, το κρυπτογραφικό σχήμα δημόσιου κλειδιού RSA, τρόποι δημιουργίας του ζεύγους κλειδιών, αλγόριθμος κατασκευής τυχαίων πρώτων αριθμών, αλγόριθμος γρήγορης ύψωσης σε δύναμη και υπολογισμού υπολοίπου από διαίρεση. Αλγόριθμοι παραγοντοποίησης μεγάλων σύνθετων αριθμών (Pollard ρ, Pollard p-1, Dixon's random squares).

Κρυπτογραφικό Σύστημα ElGamal στο Zp*. Το πρόβλημα του Διακριτού Λογάριθμου σε πολλαπλαστική ομάδα. Αλγόριθμοι επίλυσης του Διακριτού λογάριθμου: Αλγόριθμος του Shank (Baby-Step-Giant-Step), αλγόριθμος του Pollard Rho, αλγόριθμος των Pohling-Hellman και ο αλγόριθμος Index Calculus.

Κρυπτογραφικά συστήματα ElGamal σε ελλειπτικές καμπύλες. Τι είναι οι ελλειπτικές καμπύλες, κατασκευή ασφαλών ελλειπτικών καμπυλών, βασικές αλγεβρικές πράξεις και αλγόριθμοι υλοποίησής τους. Το πρόβλημα του διακριτού λογαρίθμου στις ελλειπτικές καμπύλες.

Προτεινόμενα συγγράμματα:

1. Guide to Elliptic Curve Cryptography, Darrel Hankerson, Alfred Menezes, Scott Vanstone, Springer.
2. Cryptography: Theory and Practice, Douglas Stinson, Chaplman & Hall/CRC.
3. Σύγχρονη Κρυπτογραφία: Θεωρία και Πράξη, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας, Παπασωτηρίου.