

תאריך עדכון: י' בתמוז תשס"ט

## אלגברה יישומית (88374)

סוג הקורס: הרצאה

שנת לימודים: תשס"ט סמסטר: ב' היקף שעות בשבוע: 3

אתר הקורס:

[http://www.math.biu.ac.il/~radin/courses/88374\\_applied\\_algebra/88374.htm](http://www.math.biu.ac.il/~radin/courses/88374_applied_algebra/88374.htm)

### א. מטרת הקורס:

הכרת יישומים של אלגברה מודרנית (בעיקר חבורות ושדות) ומתמטיקה בדידה.

### ב. תוכן הקורס:

#### נושאי הקורס:

כפל פולינומים מהיר בעזרת FFT, שימושים של פונקציות יוצרות, קודים לתיקון שגיאות, יסודות תורת הצפינה.

#### תכנית הוראה מפורטת:

1. כפל פולינומים מהיר בעזרת FFT: יסודות בסיבוכיות אלגוריתמים, כפל פולינומים נאיבי, שיטת "הפרד ומשול" (לפי שיטת גאוס להכפלת שני מספרים מרוכבים בעזרת 3 הכפלות של ממשיים).
2. שורשי יחידה, הצגת פולינום על-ידי מקדמים ועל-ידי ערכים, התמרת פוריה בדידה (DFT), מימוש על-ידי FFT, שימוש ב-FFT להכפלה מהירה של פולינומים.
3. דמיון ושוני בין התמרת פורייה רציפה ובדידה – דואליות בחבורות אבליות.
4. יישומים של פונקציות יוצרות: "מחשבת" בלוח אינסופי.
5. תורת הקידוד: ערוץ בינרי סימטרי, מרחק המינג, קוד לתיקון שגיאות, חסמים לגודל הקוד: המינג, סינגלטון, גילברט-ורשמוב.
6. קודים ליניאריים: מטריצה יוצרת ומטריצת בדיקת זוגיות, קוד דואלי, קודים שקולים, דוגמאות של קודים (ליניאריים ולא ליניאריים), פענוח בעזרת תסמונת (סינדרום).
7. קודים ציקליים: רקע על חוגים, חוג הפולינומים כתחום אידיאלים ראשיים (PID), קוד ציקלי כאידיאל, הפולינום היוצר, דוגמאות (כולל קודי המינג וגולאי), קידוד ופענוח באמצעות הפולינום היוצר, קודים מושלמים.
8. קודי BCH: רקע על שדות סופיים, איבר פרימיטיבי ופולינום פרימיטיבי, הגדרת קוד BCH, דוגמאות, מרחק מתוכנן ומרחק אמיתי, קודי ריד-סולומון.
9. תורת הצפינה: רקע בתורת המספרים, בעיות "קשות": פירוק לראשוניים, הוצאת לוגריתם בדיד. הצפנה עם מפתח ציבורי, עם דגש על El-Gamal, RSA.

### ג. חובות הקורס:

דרישות קדם: 88195, 88211.

חובות / דרישות / מטלות: בחינת סיום, תרגילי בית. חובה להגיש לפחות 80% מהתרגילים.

מרכיבי הציון הסופי: 90% בחינת סיום, 10% ציון הגשת תרגילים.

**ד. ביבליוגרפיה:**

1. Cormen, Leiserson, Rivest and Stein, ***Introduction to Algorithms***, 2<sup>nd</sup> Ed., 2001.
2. Hoffman, Leonard, Lindner, Phelps, Rodger and Wall, **Coding Theory: The Essentials**, 1991.
3. Lidl and Pilz, ***Applied Abstract Algebra***, 2<sup>nd</sup> Ed., 1998.
4. Nagpaul and Jain, ***Topics in Applied Abstract Algebra***, 2005.
5. Stinson, **Cryptography: Theory and Practice**, 2<sup>nd</sup> Ed., 2002.