מבוא לתורת המספרים

מרצה: דן לוי

א. מטרות הקורס ותכניו

תורת המספרים היא אחד הענפים המרתקים ביותר של המתמטיקה. מצד אחד שורשיה הם בשחר התרבות, ומצד שני יש לה שימושים פרקטיים חשובים ומגוונים בהווה, בין היתר במדעי המחשב, כבסיס לשיטות הצפנה וזיהוי חדישות. כיום, הכרה והבנה של מושגים ותוצאות בסיסיים בתורת המספרים היא הכרח לכל מי שמעוניין להבין מימושים של פרוטוקולים קריפטוגרפיים לאבטחת מידע ברשתות תקשורת. מטרות הקורס הן:

1. לימוד שיטתי של מושגים ותוצאות מתורת המספרים האלמנטרית.
2. הכרת הצד האלגוריתמי של תורת המספרים.
3. הכרת תוצאות שימושיות לקריפטוגרפיה.

ב. שיטת ההוראה

ההוראה תתבסס על הרצאות פרונטליות ועל עבודה עצמית בפתרון תרגילים שיחולקו במהלך הקורס. ההרצאות יכללו הגדרות והוכחות של תוצאות מסורתיות מתורת המספרים היסודית, ומספר תוצאות מתורת המספרים המתקדמת, ללא הוכחה. כמו כן נדון בבעיות אלגוריתמיות הקשורות במימוש הפרקטי של הרעיונות התיאורטיים. מטרת התרגילים היא להמחיש את הרעיונות והתוצאות שיוצגו בהרצאה, להרחיבם ולתרום להפנמתם.

ג. דרישות קדם

ציון עובר בקורסים: מבוא ללוגיקה ותורת הקבוצות, מתמטיקה בדידה, חדו"א, אלגברה ליניארית 1, מבוא להסתברות ומבוא למדעי המחשב.

במקרים מיוחדים ובאישור המרצה, ניתן יהיה לאשר חריגה מדרישות אלה.

ד. נושאי הלימוד

1. חילוק שלמים, מספרים ראשוניים ומורכבים, מבחן ראשוניות באמצעות חילוק, סינון ראשוניים באמצעות נפת ארתוסטנס. בעית הפקטוריזציה וחשיבותה לקריפטוגרפיה.
2. חילוק עם שארית ומחלק משותף מקסימלי. האלגוריתם של אויקלידס לחישוב המחלק המשותף המקסימלי, האלגוריתם המורחב של אויקלידס, ניתוח יעילות האלגוריתם של אויקלידס. תכונות של המחלק המשותף המקסימלי. כפולה משותפת מינימלית. פתרון משוואה דיופנטית ליניארית בשני משתנים.
3. משפט הפירוק הראשוני.
4. התפלגות הראשוניים, וצפיפות הראשוניים בתוך הטבעיים.
5. פונקציות אריתמטיות כפליות. סכום מחלקים ומספרם.
6. מספרי מרסן, מספרים מושלמים ומספרי פרמה.
7. חשבון מודולרי: קונגרואנציות ותכונותיהן היסודיות. הכרת האלגוריתם להעלאה בחזקה מודולרית. פתרון קונגרואנציות ליניאריות.
8. משפט השאריות הסיני ושימושיו.
9. מושג החבורה ומספר תוצאות יסודיות מתורת החבורות שיש להן שימוש בתורת המספרים, כגון תכונות של חבורות ציקליות סופיות.
10. המשפט הקטן של פרמה, משפט אוילר, ותכונות פונקצית אוילר.
11. שורשים פרימיטיביים וקיומם. משפט גאוס על סיווג המספרים הטבעיים שיש להם שורש פרימיטיבי. מציאת יוצר בחבורה ציקלית.

הערה: יתכנו שינויים ועדכונים ברשימה הנ"ל בהתאם לקצב הלימוד בפועל.

ה. ביבליוגרפיה

הוראת הקורס אינה צמודה לסדר ולתכנים של ספר לימוד מסוים. עם זאת קיימים ספרים רבים העוסקים בתורת המספרים האלמנטרית וביישומיה, ומכסים את מרבית נושאי הלימוד ברמה הנדרשת. ספר לימוד בעברית (מתורגם מאנגלית) שנמצא בספרית המכללה:

דיוויד מ. ברטון, תורת המספרים האלמנטרית, הוצאת האוניברסיטה הפתוחה, מהדורה חמישית.

ו. הגשת תרגילים וקביעת ציון התרגילים

התלמידים יקבלו באופן סדיר דפי תרגיל במהלך הסימסטר, לתרגול עצמי של החומר הנלמד בהרצאות ובתירגול. פתרון סדיר של תרגילים הוא מרכיב מהותי ביותר בלימוד הקורס ותנאי הכרחי להצלחה בו. על התלמידים להקפיד הקפדה יתרה שלא לחרוג ממועדי ההגשה שנקבעו. את התרגילים יש לפתור בהתאם לחומר שנלמד בהרצאות ובתרגילים עד למתן אותו תרגיל. כל תרגיל אשר יוגש במועד שנקבע ייבדק ויקבל ציון. על התלמידים להגיש את התרגילים בצורה קריאה ומסודרת ולפי ההנחיות המפורטות. בודק התרגילים יהיה רשאי לפסול הגשה של תרגילים שיכתבו בצורה רשלנית ובלתי קריאה. הקפידו לשמור ברשותכם עותק של כל תרגיל שאתם מגישים.

ציון כל תרגיל הוא 1 (עובר) או 0 (נכשל). תרגיל שאינו מוגש במועד ציונו אפס. ציון התרגילים הכולל הוא סכום ציוני התרגילים הבודדים. כדי לא להיכשל בקורס, ציון התרגילים הכולל חייב להיות לפחות 6.

הערות:

1. חובת הגשת התרגילים חלה על כלל תלמידי הקורס, כולל תלמידים שחוזרים עליו. תלמידים אלה חייבים לפתור מחדש את התרגילים ולהגישם כמו כל תלמיד אחר.
2. לא כל התרגילים המוגשים בהכרח ייבדקו, ולא תנתן הודעה מראש האם תרגיל שהוגש יבדק או לא. תרגילים לא בדוקים אינם משתקללים בציון התרגילים הסופי, ולכן **חשוב להקפיד ולהגיש את כל התרגילים**.

ז. בחינת הסיום

בסיום הקורס תתקיים בחינה מסכמת על החומר הנלמד, במועדים שיקבעו לכך על-ידי המכללה. הנחיות מדויקות לגבי היקף החומר לבחינה ומתכונתה תימסרנה בסמוך למועד תום הסימסטר.

ח. חובות הקורס וקביעת הציון הסופי

חובות הקורס: ציון בחינה 60 ומעלה, וצבירת 6 נקודות לפחות בציוני התרגילים. הציון הסופי הוא ציון הבחינה.