בס"ד

מכללה ירושלים

קורס 35210.1.1 תורת המספרים לתואר שני

תשפ"ג סמסטר ב'

(המרצה ד"ר ודים זאב אוסטפנקו)

Syllabus

1. משפט החלוקה עם שארית)חלוקה אוקלידית(
2. מספרים ראשוניים והמשפט היסודי של האריתמטיקה)פירוק לגורמים(
3. מחלק משותף מרבי)ממ"מ(ומספרים זרים
4. מבוא לאריתמטיקה מודולרית
5. מבנים אלגבריים מודולריים: פעולות חיבור וכפל
6. איברים הפיכים מודולריים ומציאת הפכים
7. פונקציית Euler φ וחישוב מספר האיברים ההפיכים
8. חזקות מודולריות, מחזוריות ומשפט Euler
9. אלגוריתם חישוב מהיר: העלאה בחזקה באמצעות ריבועים חוזרים
10. מערכת הצפנה מפתח ציבורי: פרוטוקול RSA
11. תהליכי הצפנה, פענוח וסיכום הקורס

מידע נוסף

אתר הקורס: http://www.vzostapenko.org/academiah.html

ואר אלקטרוני: ostap@math.biu.ac.il

בס"ד

ספרות מומלצת

(ישנם עותקים בספריה)

דיוויד מ. ברטון, תורת המספרים האלמנטרית, פרקים: 2.1–2.4, 3.1–3.2, 4.1, 4.2, 4.4, 5.1–5.2, 7, 10.1

מרכיבי הציון הסופי

מבחן סוף הקורס: 80%

תרגילי בית: 20%

חשוב ! הסטודנט מקבל ציון סופי של הקורס רק בתנאי שציונו עבור מבחן מסכם לא נמוך מ־55 וגם בתנאי נוסף שהציון הסופי לא נמוך מ־60

בהצלחה!