מבחן בתורת המספרים האלגוריתמית

תאריך: 07.02.2019
מספר קורס: 2-7017410-1, 2-7017410-2
שנה אקדמית: תשע"ט
סמסטר: א
מועד: א
מרצה: ד"ר אלעד אייגנר-חורב
מחלקה: מדעי המחשב
פקולטה: מדעי הטבע
משך: 3 שעות
חומר עזר שמותר להכניס לבחינה: מחשבון בלבד. כל דבר אחר הינו אסור.
מבנה המבחן: 3 שאלות ללא בחירה

הנחיות נוספות:

1. הבנת הנקרא הינה חלק מן המבחן. לא ניתן לבקש הסבר או הקראה של שאלות מסגל הקורס במהלך המבחן.
2. תשובותיכן חייבות להיות מאורגנות היטב וקריאות. נקודות לא תוענקנה לתשובות שאין הסגל מצליח לקרוא ולהבין.
3. תשובות שאורכן ייקבע על ידי הסגל כלא סביר ביחס לשאלה הנתונה לא תיתקבלנה. גם אם התשובה נכונה ואורכה לא סביר לפי דעת הסגל יש לסגל את שיקול הדעת לדחות אותה. תשובות נכונות שאינן "יעילות" במובן שאלו מתעלמות מהכלים שנלמדו ופשוט שוקלות את כל המיקרים באופן "עיוור" לא תיתקבלנה. שיקול הדעת שמור לסגל כמובן.
4. תוכן שמופיע בדף שכתוב עליו "טיוטה" לא ייבדק. ולהיפך, תוכן שלא מופיע עליו "טיוטה" ייבדק באופן מלא. הקפידו לנהל את דפי הטיוטה במבחנכם כראוי ובצורה ברורה.
5. לכל שאלה יש לספק הוכחה מלאה אלא אם כן נאמר במפורש אחרת בגוף השאלה הנתונה.
6. כל תשובה חייבת להיות מבוססת על החומר שנלמד בקורס. לא ניתן להישתמש במשפטים ותוצאות חזקות יותר שלא הוכחו במהלך הקורס ולהסיק מהם בנקל את התשובה. ההתייחסות לגישה שכזו הינה עיקור השאלה מתוכן.
7. בשאלות חישובים יש להסביר במפורט כל מעבר בחישוב. בשום אופן לא תתקבל תשובה שמכילה רק תשובה סופית ולא יתקבלו חישובים ללא הסבר מלא של כל מעבר בחישוב.
8. הפניות:
   a. באופן כללי ניתן להשתמש בכל תוצאה שנלמדה במהלך הקורס בהרצאות ובתרגולים בלבד. עם זאת ישנן הגבלות על הפניות במקרים בהם נאמר במפורש בגוף שאלה נתונה שאין להפנות או אם הפנייה מעקרת את השאלה מתוכן. למשל, כאשר בשאלה נדרש להוכיח תוצאה מסויימת אזי לא ניתן להפנות אליה בטענה שזו נלמדה וזאת גם אם לא נאמר במפורש שאין לבצע הפנייה בגוף השאלה.
   b. לא ניתן להפנות לתוצאות שהיו בעבודות הקורס.
   c. יש שתי דרכים בלבד לביצוע הפנייה. הראשונה הינה לציין את שם המשפט בו אתם מעוניינים להישתמש במידה ולמשפט אכן יש שם שמזהה אותו באופן בלעדי. השנייה נוגעת למשפטים ותוצאות ללא שם מזהה ייחודי עבורם. במקרה זה יש לנסח באופן מלא תקין ונכון את המשפט שאתם טוענים שנלמד בהרצאות ו/או התירגולים ולהפנות לניסוח הזה מתוך שאר חלקי התשובה.
   d. אין להפנות לחלקי הוכחות של תוצאות שנלמדו בקורס.
   e. ניתן להפנות לכל סעיף ושאלה בגוף המבחן גם אם לא פתרתם את אלו. יש להקפיד שהשאלה או הסעיף במבחן אליהם אתם מפנים מאפשרים הפנייה אליהם וכי הפנייה אליהם הינה משמעותית (לא ניתן להפנות לשאלות שמבקשות הוכחה או הפרכה).
   f. לא ניתן להפנות לחלקי תשובות שסיפקתם לשאלות או סעיפים אחרים. כל תשובה חייב שתהיה מוכלת בתוך עצמה או מלווה בהפניות ראויות שיאפשרו את הבנתה.
   g. סגל הקורס לא יענה לשאלות במהלך המבחן לגבי האופן בו יש לבצע הפניות. עליכם להסיק לבד אם ההפניה שביצעתם תואמת את ההוראות לעיל או לא.
9. במקרה של חשד של הסגל למעשה רמייה שומר הסגל לעצמו את הזכות לעכב ציון ולנהל מבחן פרונטלי שעל פי מבחן זה יינתן הציון או ייקבע שיש להמשיך טיפול בוועדת משמעת. זוהי החלטה של הסגל אם לקיים מבחן פרונטלי שכזה.

בהצלחה!

שאלה 1: בקיאות בסיסית בחומר הקורס ללא הוכחות - 60 נקודות

סעיף 1: (10 נקודות) הגדירו מהו מספר קרמייקל.

סעיף 2: (10 נקודות) נסחו את משפט השאריות הסיני ללא הוכחה.

סעיף 3: (10 נקודות) הגדירו את הפונקציה φ של אוילר.

סעיף 4: (10 נקודות) נסחו את משפט אוילר ללא הוכחה. הכוונה למשפט שמשתמש בפונקציה φ.

סעיף 5: (10 נקודות) הראו הרצה מלאה של אלגוריתם אוקלידס על מנת לחשב (2260,816).

סעיף 6: (10 נקודות) הראו הרצה מלאה של אלגוריתם אוקלידס המורחב על מנת למצוא שלמים m ו n כך ש

$$(2260,816) = m \cdot 2260 + n \cdot 816$$

שאלה 2: בקיאות בהוכחות מההרצאות, תירגולים, דפי חזרה, ועבודות + יכולת הרכבה - 30 נקודות

סעיף 1: (7 נקודות) נסחו את משפט האינדוקציה החלשה ואת משפט האינדוקציה החזקה. הוכיחו כי משפט האינדוקציה החלשה גורר את משפט האינדוקציה החזקה באופן ישיר, כלומר ללא שימוש ב WOP (דהיינו עיקרון הסדר הטוב).

- בסעיף זה במידה וניסוח אי אלו מהמשפטים המצויינים לעיל שגוי ההוכחה לא תיבדק.
- בידקו היטב שאתם מוכיחים את הכיוון הנכון בגרירה שכן הכיוון השני (שלא נדרש כאן) הינו טריוויאלי.

סעיף 2: (10 נקודות)

א. (4 נקודות) יהיו $a,b \in \mathbb{Z}^+$. הוכיחו כי $(a,b) \cdot lcm(a,b) = a \cdot b$.

ב. (6 נקודות) יהיו $a_1, a_2, \ldots, a_n$ מספרים שלמים חיוביים זרים. הוכיחו כי $lcm(a_1, a_2, \ldots, a_n) = \prod_{i=1}^{n} a_i$.

- הבהרה לגבי שימוש בהפניות בסעיף ב': טענה זו הוכחה בתירגול וההוכחה שהוצגה בתירגול הורכבה ממספר טענות עזר. כל טענת עזר שהופיעה בהוכחה בתירגול ושאינה נמצאת בטופס המבחן, לא ניתן להפנות אליה במסגרת התשובה לסעיף זה ללא ניסוח מלא +הוכחה מלאה שלה.

סעיף 3: (8 נקודות) להלן פסודוקוד של אלגוריתם המסננת של ארסטות'נס.

```
SIEVE(n):

 for k=2 to n do : A[k]=1

 for k=2 to ⌊√n⌋ do:

          if A[k]=1 then:
               i=2k
               while i≤n do:
                    A[i]=0
                    i=i+k
```

הוכיחו כי בסיום האלגוריתם A[k] = 1 אם ורק אם k הינו מספר ראשוני. חובה לענות באמצעות טענות נשמרות ללולאות.

(המשך שאלה 2)

סעיף 4: (5 נקודות - בחינת יכולת הרכבה) בשאלה 1 ניסחתם את משפט השאריות הסיני. המשפט טוען לקיום וייחודיות של פתרון למערכת קונגרואנציות מסויימת. הוכיחו כעת את החלק של משפט השאריות הסיני הטוען לקיום פתרון באמצעות משפט אוילר שגם אותו ניסחתם בשאלה 1.

- אין צורך להוכיח את הייחודיות של הפתרון.
- אם הניסוחים שסיפקתם למשפט השאריות הסיני או משפט אוילר בשאלה 1 שגויים או מי מהם כלל לא קיים אזי תשובתכם בסעיף זה לא תישקל.

שאלה 3: יצירתיות והפנמה - 10 נקודות

יהיו $a,m\in\mathbb{Z}^+$ כך ש $(a,m)=1$. הוכיחו כי אם $a^{m-1}\equiv 1\,(m)$ וגם $a^x\not\equiv 1\,(m)$ לכל $x\in\mathbb{Z}^+$ כך ש $x\,|\,m-1$ וגם $x<m-1$ אזי m ראשוני.

<u>הצעה:</u> האם קיים מספר חיובי קטן ביותר d שמקיים $a^d\equiv 1\,(m)$?

בהצלחה!