מבחן בתורת המספרים האלגוריתמית

תאריך: 25.02.2019
מספר קורס: 2-7017410-1, 2-7017410-2
שנה אקדמית: תשע"ט
סמסטר: א
מועד: ב
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 את המושג הופכי מודולארי.

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

סעיף 3: (10 נקודות) נסחו את משפט Wilson ללא הוכחה.

סעיף 4: (10 נקודות) הגדירו את המושג מערכת שאריות מצומצמת מודולו n.

סעיף 5: (10 נקודות) הראו הרצה מלאה של אלגוריתם אוקלידס על מנת לחשב (172,20).

סעיף 6: (10 נקודות) קיבעו כי קיימים x ו y שלמים כך שאלו מקיימים $172x+20y=1000$ מבלי לחשב x ו y ספציפיים. לאחר מכן ספקו נוסחה לכל הפתרונות האפשריים למשוואה מה שבפרט אומר כי עליכם לחשב לפחות פתרון אחד באמצעות אלגוריתם Euclid המורחב. יש להסביר ולספק הצדקות לכל מעבר.

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

סעיף 1: (7 נקודות) יהיו $a,n\in\mathbb{Z}^+$ כך ש: $(a,n)=1=(a-1,n)$. הוכיחו כי $\sum_{j=1}^{\varphi(n)} a^{j-1}\equiv 0\ (n)$.

סעיף 2: (10 נקודות) נסחו את אלגוריתם RSA וציינו מה יהיו P_A ו S_A בסוף האלגוריתם. נסחו את הטענה עבור P_A ו S_A שקובעת את נכונותו של האלגוריתם והוכיחו אותה.

סעיף 3: (8 נקודות) נסחו את בעיית הפעילויות. תארו אלגוריתם רקורסיבי עבור בעיה זו. ספקו הוכחת נכונות עבור האלגוריתם שכתבתם. בשאלה זו לא ניתן להפנות לשום טענה שהוכחה בכיתה (כאמור בשיעור החזרה) בנוגע לבעיה זו ויש להוכיח הכל במסגרת המבחן.

סעיף 4: (5 נקודות - בחינת יכולת הרכבה) הוכיחו כי יש אינסוף פסודו-ראשוניים מבסיס 2.

שאלה 3: יצירתיות והפנמה - 10 נקודות

מספר $n\in\mathbb{Z}^+$ יקרא square-free אם לא קיים ראשוני p כך ש $p^2\mid n$. הוכיחו כי אם n פריק וגם $\varphi(n)\mid n-1$ אזי n הינו square-free ובעל לפחות 3 פקטורים שונים.

בתשובתכם לשאלה זו שימו לב היטב לשימוש בהנחה שהמספר פריק. שכן אכן מספר ראשוני מקיים הכל ממה שנאמר לעיל פרט לכך שאין לו לפחות 3 פקטורים שונים.

בהצלחה!