מבחן בתורת המספרים האלגוריתמית

תאריך: 12.02.2018
מספר קורס: 2-7017410-1, 2-7017410-3
שנה אקדמית: תשע"ח
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 לא גרפי בלבד. כל דבר אחר הינו אסור.
מבנה המבחן: 3 שאלות ללא בחירה + נוסח מקביל של המבחן באנגלית מצורף

הנחיות נוספות:

1. הבנת הנקרא הינה חלק מן המבחן. אין לפנות לסגל הקורס במהלך הבחינה על אף נושא פרט למקרה שבו הסטודנט/ית חושב/ת שמצא/ה טעות במבחן. אין לבקש הסבר או הקראה של שאלות מסגל הקורס במהלך המבחן.
2. המתרגלים אינם רשאים לענות על אף שאלה משום סוג שהוא במבחן. טענות לקבלת הנחיות ממתרגלים וכי אלו השפיעו במידת מה על התשובה במהלך הבחינה לא תכובדנה בעת הבדיקה.
3. תשובותיכן חייבות להיות מאורגנות היטב וקריאות. נקודות לא תוענקנה לתשובות שאין הסגל מצליח לקרוא ולהבין.
4. תשובות באורך שהסגל יקבע שאורכן איננו סביר לשאלה הנתונה לא תיתקבלנה. גם אם התשובה נכונה ואורכה לא סביר יש לסגל את שיקול הדעת לדחות אותה.
5. 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.
6. בשאלות הוכחה יש לספק הוכחה מלאה אלא אם כן נאמר במפורש אחרת.
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. ניתן להשתמש בכל תוצאה שנלמדה במהלך הקורס אם בהרצאות, בתרגולים, או דרך קובץ ההרצאות שסופק באתר הקורס.
   b. השימוש בתוצאות לעיל מותנה בהפניה ראויה לתוצאה שנלמדה וכמובן במידה וזו לא מעקרת את השאלה מתוכן למשל אם בשאלה נדרש להוכיח את התוצאה המדוברת.
   c. על מנת לבצע הפנייה יש או לספק את המספר הסידורי של התוצאה בקובץ ההרצאות או לנסחה באופן מלא בגוף התשובה במקום ראוי ואז להפנות אליה במהלך תשובתכם.
   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.
   f. לא ניתן להפנות לחלקי תשובות שסיפקתם לשאלות או סעיפים אחרים. כל תשובה חייב שתהיה מוכלת בתוך בעצמה 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 ייתן הציון או ייקבע שיש להמשיך טיפול בוועדת משמעת. זוהי החלטה של הסגל אם לקיים מבחן פרונטלי שכזה.

בהצלחה!

נוסח 1: עברית (נוסח באנגלית מצורף למטה)

שאלה 1: (40 נקודות)

א. (2 נקודות) הגדירו סמל Legendre.

ב. (3 נקודות) נסחו את הקריטריון של Euler (ניסוח בלבד ללא הוכחה).

ג. (3 נקודות) נסחו את המשפט של Gauss עבור סמלי Legendre (ניסוח בלבד ללא הוכחה).

ד. (3 נקודות) נסחו את משפט ה- Quadratic reciprocity (ניסוח בלבד ללא הוכחה).

ה. (3 נקודות) נסחו את משפט השאריות הסיני (ניסוח בלבד ללא הוכחה).

ו. (13 נקודות) הוכיחו את משפט Gauss שניסחתם בסעיף ג' לשאלה זו. (אם הניסוח שסיפקתם למשפט זה בסעיף ג' לשאלה זו שגוי ההוכחה שתספקו כאן לא תתקבל – בדקו את סעיף ג' היטב)

ז. (13 נקודות) יהי p ראשוני אי-זוגי שאיננו 7. השתמשו במשפט ה Quadratic Reciprocity ובמשפט השאריות הסיני על מנת להוכיח כי:

$$\left(\frac{7}{p}\right) = \begin{cases} 1, & p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}, \\ -1, & \text{otherwise.} \end{cases}$$

שאלה 2: (40 נקודות)

א. (3 נקודות) הגדירו מהו ה gcd של שני מספרים שלמים חיוביים.

ב. (3 נקודות) ספקו ניסוח רקורסיבי לאלגוריתם של Euclid לחישוב ה gcd של שני מספרים $a \geq b > 0$ (בסעיף זה יש רק לספק את הפסודוקוד שנלמד לאלגוריתם זה).

ג. (2 נקודות) הגדירו את סדרת פיבונאצי'.

ד. (8 נקודות) הוכיחו כי האלגוריתם הרקוסיבי שסיפקתם בסעיף ב' לשאלה זו עוצר.

ה. (9 נקודות) הוכיחו כי במידה והאלגוריתם שסיפקתם בסעיף ב' עוצר אזי זה מחזיר (a,b) כפי שנדרש.

ו. (9 נקודות) נכנה בשם EUCLID(a,b) את הפרוצדורה שסיפקתם בסעיף ב' לשאלה זו. הוכיחו את הטענה הבאה: *יהיו $a > b \geq 1$ שלמים. אם EUCLID(a,b) מבצע k קריאות רקורסיביות (לא כולל הקריאה הראשונה) אזי*

$$a \geq F_{k+2} \text{ and } b \geq F_{k+1}$$

כאשר F_k מציין את המספר הפיבונאצי' ה k.

ז. (6 נקודות) כמה קריאות רקורסיביות תבצע הפרוצדורה שסיפקתם בסעיף ב' לשאלה זו על הקלט

$$a = F_{k+2} \text{ and } b = F_{k+1}$$

כאשר $k \geq 3$. יש לספק הוכחה מלאה לתשובתכם. תשובה סופית בלבד לא תתקבל.

(שאלה 3 בדף הבא)

שאלה 3: (20 נקודות)

א. (6 נקודות) יהי p ראשוני ויהי $0< k <p$ שלם. הוכיחו כי

$$(p-k)!(k-1)! \equiv (-1)^k \pmod p$$

ב. (7 נקודות) הוכיחו כי המספר

$$\left(2^{2(28n+1)}+1\right)^2+4$$

הינו פריק לכל n שלם חיובי.

ג. (7 נקודות) מספר שלם וחיובי n ייקרא square-free אם לא קיים ראשוני p כך ש $p^2 \mid n$.
הוכיחו כי אם שלם חיובי n הינו פריק ובנוסף מתקיים עבורו $\varphi(n) \mid n-1$
אזי n הינו square-free ובנוסף יש לו לפחות שלושה פקטורים ראשוניים.

בהצלחה!