מבחן בתורת המספרים האלגוריתמית

תאריך: 20.02.2020
מספר קורס: 2-7017410-1, 2-7017410-2, 2-7017410-4, 2-7017410-5
שנה אקדמית: תש"ף
סמסטר: א
מועד: א
מרצים: ד"ר אלעד אייגנר-חורב וד"ר חיה קלר
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

הוראות:

1. הבנת הנקרא הינה חלק מן המבחן. לא ניתן לבקש הסבר או הקראה של שאלות מסגל הקורס במהלך המבחן.
2. תשובותיכם חייבות להיות מאורגנות היטב וקריאות. לא תוענקנה נקודות 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:

א. 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 ההפנייה 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.

ב. לא ניתן להפנות לתוצאות שהיו במטלות הקורס. אם תרצו להשתמש באלו יש לנסחן באופן מלא ולהוכיחן באופן מלא בגוף המבחן.

ג. 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.

ד. אין להפנות לחלקי הוכחות של תוצאות שנלמדו בקורס.

ה. 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).

ו. לא ניתן להפנות לחלקי תשובות שסיפקתם לשאלות או סעיפים אחרים. כל תשובה חייב שתהיה מוכלת בתוך עצמה או מלווה בהפניות ראויות שיאפשרו את הבנתה.

ז. 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 פיו יינתן הציון או ייקבע שיש להמשיך טיפול בוועדת משמעת. זוהי החלטה של הסגל אם לקיים מבחן פרונטלי שכזה.

בהצלחה!

תזכורת: עבור $a, b \in \mathbb{Z}$ אנו מסמנים ב (a, b) את ה gcd (המחלק המשותף הגדול ביותר) של a ו b.

שאלה 1: רמת בקיאות - 60 נקודות

סעיף א: (10 נקודות) הגדירו תת-חבורה.

סעיף ב: (10 נקודות) נסחו את עיקרון הסדר הטוב (WOP).

סעיף ג: (10 נקודות) יהיו $a, b \in \mathbb{Z}$ בעלי הפקטוריזציות (הפירוק הקנוני לראשוניים) $a = \prod_{i=1}^{k} p_i^{a_i}$ ו $b = \prod_{i=1}^{k} p_i^{b_i}$. רשמו את הפקטוריזציה של (a, b).

סעיף ד: (10 נקודות) מצאו נציג קנוני עבור 3^{4101} מודולו 17. יש להסביר כל שלב בחישוב.

סעיף ה: (10 נקודות) הגדירו את הפונקציה φ של אוילר ונסחו את משפט אוילר ללא הוכחה.

סעיף ו: (10 נקודות) תהי $(G, *)$ חבורה אבלית (קומוטטיבית) סופית עם איבר נייטרלי e כך ש $G = \{g_1, \ldots, g_n\}$.
יהי $a := g_1 * g_2 * \cdots * g_n$. הוכיחו כי $a^2 = e$.

שאלה 2: רמת הפנמה - 25 נקודות

סעיף א: (7 נקודות) נסחו והוכיחו את גירסת האם ורק אם של משפט וילסון (דהיינו משפט וילסון ואת המשפט ההפוך לו).

סעיף ב: (10 נקודות) יהיו $m, n \in \mathbb{Z}^+$ כך ש $m > n$ ו $2 \le t \in \mathbb{N}$. הוכיחו כי $(t^n - 1, t^m - 1) = t^{(n,m)} - 1$.

סעיף ג: (8 נקודות)

ג.1 (4 נקודות) יהיו $a \in \mathbb{N}$ ו $2 \le n \in \mathbb{N}$. הוכיחו כי אם $a^n - 1$ ראשוני, אזי n ראשוני.

ג.2 (4 נקודות) מצאו את כל הראשוניים מהצורה $n^5 - 1$. הוכיחו את טענותיכם.

שאלה 3: רמת יצירתיות - 15 נקודות

בשאלה זו הינכם מתבקשים להוכיח את הטענה הבאה.

<u>טענה:</u>

יהי $2 \le a \in \mathbb{N}$ ויהי p ראשוני אי-זוגי כך ש $p \nmid a^2 - 1$. אזי המספר $n := \dfrac{a^{2p} - 1}{a^2 - 1}$ הינו פסודו-ראשוני לפי בסיס a.

הסעיפים הבאים מנחים אתכם בהוכחת טענה זו. אנא הביטו בהוראה 8 תת-סעיף ה' שמופיעה בהוראות המבחן בעודכם עונים על שאלה זו.

סעיף א: (3 נקודות) הוכיחו כי n המוגדר לעיל הינו שלם ופריק.

בסעיף זה הינכם יכולים להסתמך על העובדה ש $x + 1 \mid x^k + 1$ לכל $k \in \mathbb{N}$ אי-זוגי וכל $x \in \mathbb{N}$.

אין צורך להוכיח עובדה זו.

סעיף ב: (7 נקודות) יהי p ראשוני אי-זוגי כך ש $p \nmid a^2 - 1$. הוכיחו כי $p \mid n - 1$ וגם $2 \mid n - 1$.

סעיף ג: (2 נקודות) יהי p ראשוני אי-זוגי כך ש $p \nmid a^2 - 1$. הוכיחו כי $a^{2p} - 1 \mid a^{n-1} - 1$.

סעיף ד: (3 נקודות) הוכיחו את הטענה המופיעה בראש שאלה זו.

בהצלחה!