מבחן בתורת המספרים האלגוריתמית

תאריך: 04.03.2018
מספר קורס: 2-7017410-1, 2-7017410-3
שנה אקדמית: תשע"ח
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 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. (3 נקודות) הגדירו את המושג פונקציה כפלית.

ב. (3 נקודות) הגדירו את ה totient function של Euler.

ג. (3 נקודות) נסחו (ללא הוכחה) את משפט Euler והסבירו כיצד זה מכליל את משפט Fermat הקטן.

ד. (14 נקודות) הוכיחו כי ה totient function של Euler הינה כפלית (מבלי להסתמך על סעיפים במבחן ותוצאות מהקורס שמייתרים את השאלה).

ה. (2 נקודות) אם m ו n שני מספרים שלמים חיוביים מהי הפקטוריזציה של (m,n) ?

ו. (7.5 נקודות) השתמשו בסעיף ה׳ לשאלה זו על מנת להוכיח כי

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \frac{d}{\varphi(d)}$$

כאשר כאן m ו n זוג מספרים שלמים חיוביים (לא בהכרח זרים) ו d = (n,m).

ז. (7.5 נקודות) יהיו a ו b זוג מספרים שלמים וחיוביים. הוכיחו כי אם $a \mid b$ אזי $\varphi(a) \mid \varphi(b)$

את הטענה עליכם להוכיח באינדוקציה על b כאשר בצעד הינכם משתמשים בסעיף ו׳ לשאלה זו.

שאלה 2: (40 נקודות)

א. (2 נקודות) נסחו את משפט Fermat הקטן (ללא הוכחה)

ב. (2 נקודות) הגדירו את המושג פסודו-ראשוני מבסיס b.

ג. (2 נקודות) הגדירו את המושג מספר Carmichael.

ד. (4 נקודות) הוכיחו כי אם n הינו פסודו-ראשוני מבסיס a והינו גם פסודו-ראשוני מבסיס b אזי n פסודו-ראשוני מבסיס ab.

ה. (15 נקודות) הוכיחו את משפט Fermat הקטן. (שימו לב שאם הניסוח שסיפקתם למשפט זה בסעיף א׳ לשאלה זו הינו שגוי אזי ההוכחה בסעיף זה לא תיתקבל. בידקו את סעיף א׳ לשאלה זו היטב).

ו. (8 נקודות) יהי p ראשוני. השתמשו בקונגרואנציה הטריוויאלית $2^p \equiv 1 \pmod{2^p - 1}$

על מנת להוכיח כי אם $2^p - 1$ פריק אזי מספר זה הינו גם פסודו-ראשוני מבסיס 2.

ז. (7 נקודות) יהי p ראשוני. הוכיחו כי

$$\sum_{i=1}^{p-1} i^{p-1} \equiv -1 \pmod{p}$$

(שאלה 3 בדף הבא)

שאלה 3: (20 נקודות)

א. (8 נקודות) יהיו a ,b ו n שלמים חיוביים. הוכיחו כי:

$$(a^n, b^n) = (a, b)^n$$

וגם

$$\mathrm{lcm}(a^n, b^n) = \mathrm{lcm}(a, b)^n$$

ב. (6 נקודות) הוכיחו כי מספר שלם וחיובי n הינו פריק אם ורק אם $\varphi(n) \leq n - \sqrt{n}$

ג. (6 נקודות) להלן טענה של Euler:

משפט 1: יהי p ראשוני אי-זוגי ויהי a זר ל p. אם q הינו ראשוני אי-זוגי שעבורו מתקיים $p \equiv \pm q \pmod{4a}$

אזי

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

ולהלן משפט ה Quadratic Reciprocity:

משפט 2: יהיו p ו q שני ראשוניים אי-זוגיים שונים. אזי

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

הוכיחו כי משפט 1 גורר את משפט 2.

בהצלחה!

Question 1: (40 credits)

(a) (3 credits) Define the term *multiplicative function.*

(b) (3 credits) Define Euler's *Totient function.*

(c) (3 credits) State Euler's theorem (without proof) and explain how this result generalises Fermat's little theorem.

(d) (14 credits) Prove that Euler's Totient function is multiplicative. In your answer you are not allowed to use results from the course or ones stated in this exam that make this question void of meaning.

(e) (2 credits) Let m, n be two positive integers. What is the factorisation of (m, n)?

(f) (7.5 credits) Use part (e) of this question in order to prove that

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \frac{d}{\varphi(d)}$$

where here m and n are positive integers (which are not necessarily coprime) and $d = (m, n)$.

(g) (7.5 credits) Prove that if a and b are positive integers and $a \mid b$ then $\varphi(a) \mid \varphi(b)$. You are to prove this result using an induction on b where in the induction step you use part (f) of this question.

Question 2: (40 credits)

(a) (2 credits) state Fermat's little theorem (without proof).

(b) (2 credits) Define the term *pseudoprime to the base b.*

(c) (2 credits) Define the term *Carmichael number.*

(d) (4 credits) Prove that if a positive integer n is pseudoprime to both the bases a and b then it is also a pseudoprime to the base ab.

(e) (15 credits) Prove Fermat's little theorem. (Be advised that if the formulation you supplied for this theorem in part (a) of this question is wrong then the proof you supply here will be rejected; check part (a) properly).

(f) (8 credits) Let p be prime. Use the triviality $2^p \equiv 1 \pmod{2^p - 1}$ in order to prove that if $2^p - 1$ is composite then it is also a pseudoprime to the base 2.

(g) (7 credits) Let p be prime. Prove that $\sum_{i=1}^{p-1} i^{p-1} \equiv -1 \pmod{p}$.

(Question 3 appears on the next page)

Question 3: (20 credits)

(a) (8 credits) Let a, b, and n be positive integers. Prove that $(a^n, b^n) = (a, b)^n$ and that $\operatorname{lcm}(a^n, b^n) = \operatorname{lcm}(a, b)^n$.

(b) (6 credits) Prove that a positive integer n is composite if and only if $\varphi(n) \leq n - \sqrt{n}$.

(c) (6 credits) The following is a result by Euler:

Theorem 1. *Let p be an odd prime and let a be coprime to p. If q is an odd prime satisfying $p \equiv \pm q \pmod{4a}$ then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

The following is the quadratic reciprocity law:

Theorem 2. *Let p and q be two distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.*

Prove that Theorem 1 implies Theorem 2.