**מטלת מנחה (ממ"ן) 15**

**הקורס:** 20290 – אלגוריתמיקה – יסודות מדעי המחשב

**חומר הלימוד למטלה**: פרקים 12-10

|  |  |
| --- | --- |
| **מספר השאלות:** 6 | **משקל המטלה:** 6 נקודות |
| **סמסטר:** 2006ב | **מועד אחרון להגשה:** 14.7.2006 |

|  |
| --- |
| אנא שימו לב:  מלאו בדייקנות את הטופס המלווה לממ"ן בהתאם לדוגמה שלפני המטלות.  העתיקו את מספר הקורס ומספר המטלה הרשומים לעיל. |

### שאלה 1 (20 נקודות)

א. תארו אלגוריתם מקבילי הפותר בזמן פולינומיאלי את הבעיה של צביעת גרף בשלושה צבעים.

**הניחו** **שאין שיתוף** **בכתיבה**. כלומר, האלגוריתם אינו רשאי להשתמש במשתנה משותף

(משתנה ששני מעבדים או יותר יכולים לשנות את ערכו).

נתחו את זמן הריצה של האלגוריתם.

ב. הוכיחו את הטענה הבאה: אם קיים אלגוריתם מקבילי הפותר איזושהי בעיה NP-שלמה בזמן   
 פולינומיאלי ובאמצעות מספר פולינומיאלי של מעבדים, אז P=NP.

### שאלה 2 (20 נקודות)

נדון בפתרון לבעיית הקטע הקריטי עבור שני מעבדים.

הפתרון מבוסס על שימוש במשתנה משותף בשם lock, שערכו ההתחלתי 0.

להלן הפרוטוקול עבור כל אחד מהמעבדים:

(1) בצע פעולות פרטיות עד שתרצה להיכנס לקטע הקריטי;

(2) בדוק את ערכו של lock;

(3) אם lock = 0 אז בצע:

(2.1) lock ← 1;

(2.2) בצע את הקטע הקריטי;

(2.3) lock ← 0;

(2.4) חזור לשורה (1);

(4) אחרת חזור לשורה (2);

א. הסבירו מדוע הפתרון איננו נכון.

ב. נתקן את הפרוטוקול באופן הבא: לפני שורה (2.1) נבדוק פעם נוספת את ערכו של lock.

אם הערך הוא 0, אז נמשיך לשורה (2.1). אחרת – נחזור לשורה (2).

האם כעת הפתרון נכון ? הסבירו את תשובתכם.

### שאלה 3 (15 נקודות)

בשנת 2002 התגלה אלגוריתם פולינומיאלי (דטרמיניסטי) לפתרון בעיית הראשוניות.

מאמר שפורסם בעניין בעיתון "הארץ" נפתח במילים הבאות:

שלושה מדעני מחשב הודים טוענים שפיתחו שיטה חדשה, המאפשרת לקבוע אם מספר הוא ראשוני או לא. ייחודה של השיטה הוא שאפשר לבדוק באמצעותה גם מספרים גדולים מאוד, ואם היא אכן פועלת, כפי שסבורים מתמטיקאים מובילים שבדקו אותה, היא תוכל לשמש אמצעי יעיל לשבירת צפנים דיגיטליים.

חוו דעתכם על שני המשפטים המסומנים בקו בטקסט הנ"ל.

### שאלה 4 (20 נקודות)

א. הסבירו איך ממומש במערכת מפתח-ציבורי מנגנון של חתימה אלקטרונית.

ב. מהן כל הדרישות ממנגנון של חתימה אלקטרונית ?

האם דרישות אלה מתמלאות במערכת מפתח-ציבורי ?

נמקו את תשובתכם, תוך התייחסות לכל אחת מהדרישות שציינתם.

### שאלה 5 (15 נקודות)

איה רוצה ללמוד לטוס. כדי להתקבל לקורס, עליה לשכנע את בועז, המדריך הראשי, שהיא

איננה עיוורת-צבעים (כלומר, שהיא מסוגלת להבחין בין צבע ירוק לצבע אדום). תארו פרוטוקול הוכחה, שיאפשר לבועז להשתכנע בהסתברות הגדולה מ-0.999 שאיה איננה עיוורת-צבעים.

**שאלה 6 (10 נקודות)**

כאשר נשאל קלוד שאנון (1916-2001), אבי תורת האינפורמציה, אם מכונות יכולות לחשוב הוא השיב: "ועוד איך! אנחנו מכונות ואנחנו חושבים, לא?"

חוו דעתכם על תשובתו של שאנון.

http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Shannon.html