

מבוא לתורת המספרים למדעי המחשב (89-256)

מרצה: ד"ר מיכאל משה שיין

תש"ע סמסטר ב'

מבחן מסכם, מועד ב'

יש לענות על ארבע שאלות. במקרה שתפתרי יותר, יש לציין איזה שאלות את/ה רוצה שתיבדקנה. מותר להשתמש במחשבון פשוט, פרט לשאלות שאוסרות שימוש במחשבון. יש לנמק באופן מלא את כל הטענות שלך. משך הבחינה: שעתיים.

1. המספר 13381 הינו ראשוני. האם יש פתרון למשוואה

$$x^2 + 30x + 218 \equiv 0 \pmod{13381}$$

2. ידוע כי  $N$  הינו המכפלה של שני מספרים ראשוניים. ידוע שהפתרונות של המשוואה

$$x^2 \equiv 547 \pmod{N}$$

הינם 74, 763, 880, ו-1569 מודולו  $N$ . למצוא את  $N$  ואת הגורמים הראשוניים של  $N$ .

3. למצוא את כל הפתרונות למשוואה

$$x^7 \equiv 1 \pmod{9075}$$

רמז: כדאי לחשב את  $\varphi(9075)$ .

4. למצוא את כל מספרי קרמייקל מן הצורה  $7 \cdot 23 \cdot q$ , כאשר  $q > 23$  ראשוני.

5. למצוא את שני הספרות האחרונות (בבסיס 10) של  $613^{5770}$ .