האוניברסיטה העברית בירושלים
החוג למתמטיקה

מבחן בתורת המספרים וקריפטוגרפיה (80611)

מועד ב' תשס"ח
המורה: פרופ' א. לובוצקי

תאריך: 29/9/08
משך הבחינה: שעתיים

ענה על 5 מתוך 8 השאלות הבאות:

1. הוכח: אם p ראשוני אזי $(p-1)! \equiv -1 \pmod{p}$.

2. עבור אלו $n \in \mathbb{N}$ בחבורה $\left(\mathbb{Z}/_n \mathbb{Z}\right)^*$ יש יותר מ-2 פתרונות למשוואה $X^2 \equiv 1 \pmod{n}$? הוכח!

3. פתור את מערכת המשוואות:

$$\begin{cases} X^2 \equiv 5 \pmod{39} \\ 5X + 2 \equiv 3 \pmod{7} \end{cases}$$

אם אין פתרון, הוכח! אם יש, מצא אותו.

4. קבע עבור אלו ראשוניים p , 7 הוא שארית ריבועית.

5. הגדר מספר Carmichael והוכח שאם $p \neq 2$ ראשוני , $p^2 \mid n$, אזי n אינו מספר Carmichael .

6. חושם פרסם את המפתח הצבורי שלו $n = 209$ ו- $e = 7$. ראובן שלח לחושם את ההודעה $y = 177$ בשיטת RSA. שמעון הצליח לפצח את $(n = 19 \cdot 11)$ ולכן לפצח את המסר הסודי x .

(5 נק') א. בטא את y בעזרת x .

(8 נק') ב. בטא את x בעזרת y .

(7 נק') ג. מצא את x .

7. קבע עבור אלו מספרים טבעיים n , יש פתרון לא טריויאלי למשוואה $X^3 \equiv 1 \pmod{n}$.

8. חשב (i) $3^{10,000} \pmod{209}$

(ii) $\left(\frac{159}{851}\right)$

בהצלחה!