האוניברסיטה העברית בירושלים

החוג למתמטיקה

מבחן בקורס "תורת המספרים ושימושים לקויפאגריפיה" תשס"ח

המורה: פרופ' אלכס לובוצקי

משך הבחינה: שעתיים

24/8/08

ענה על 5 מתוך 8 השאלות הבאות:

1. הוכח שיש אינסוף ראשוניים מהצורה $6h+5$.
2. נסמן $\vartheta(x)=\sum_{p\le x}\log p$. הוכח: $\vartheta(x)\le 4x$ עבור $x\gg 0$.
3. יהא p ראשוני של פרמה (ז"א p מהצורה $p=2^n+1$; יתר על כן ראינו ש n חייב להיות חזקת-2, $n=2^t$). הוכח ש-3 איבר פרימיטיבי מודולו p
4. חושם ביקש מחבריו לשלוח לו הודעות בשיטת רבין, תוך שמוש ב $n=209$. חברו רצה לשלוח לו מספר סודי x השתמש בשיטה ושלח לי 177. מצא את 4 האפשרויות עבור x.
5. חשב א) $\left(\frac{401}{757}\right)$ ב) $d=(401,757)$ ג) הבע את d $401x+757y=d$ (ז"א מצא את x ו- y)
6. האם ב- $\left(\mathbb{Z}/1872\mathbb{Z}\right)^*$ יש איבר מסדר 4? אם כן,מצא אותו אם לא, הוכח.
7. פתור את מערכת המשוואות

$$\begin{cases}3x+5\equiv 0(31)\\ 2x+4\equiv 0(5)\\ 2x+1\equiv 0(3)\end{cases}$$

8. מצא איבר פרימיטיבי מודולו 3^7

מותר להשתמש בכל מה שלמדנו בכיתה).

בהצלחה