מבחן בתורת המספרים לתלמידי פרופ' זאב רודניק

סמסטר א' תשע"א

מועד א' 2.2.2011

<u>הוראות:</u> משך הבחינה 3 שעות.
יש לענות על כל השאלות.
אין להשתמש בחומר עזר.
ניתן להשתמש במחשבון.

1. מצאו פתרון מודולו 119 של מערכת הקונגרואנציות $\begin{cases} x = a \bmod 7 \\ x = b \bmod 17 \end{cases}$.

2. מצאו את הפירוק לאי-פריקים בחוג השלמים של גאוס **Z[i]** של המספר 11-**7i** **(i=√-1) .**

3. יהא p ראשוני המקיים $p = 2 \bmod 13$. הראו שאין פתרון לקונגרואנציה $x^2 - 8x + 3 = 0 \bmod p$.

4. מצאו את כל הפתרונות של משוואת PELL האי-זוגית $x^2-130y^2= -1$.

5. בשיטת RSA, בוחרת אליס שני ראשוניים שונים q,q' , מחשבת את מכפלתם N=qq', את פונקצית אוילר φ(N) ובוחרת מפתח הצפנה e זר ל φ(N). היא מפרסמת את N ואת e ושומרת בסוד את שאר הנתונים. כדי לשלוח לאליס מסר מוצפן , שהוא מספר P בין 0 ל N-1, מבצע בוב את החישוב הבא: $C=P^e \bmod N$ ושולח את C. איך תמצא אליס את המסר המקורי P ? נמקו.

6. יהא p ראשוני, $p=5 \bmod 8$ ו- a שארית ריבועית מודולו p : $\left(\frac{a}{p}\right) = +1$

א. הראו ש $a^{(p-1)/4} = \pm 1 \bmod p$.

ב. הראו שאם $a^{(p-1)/4} = +1 \bmod p$ אזי $x = a^{(p+3)/8}$ פותר את הקונגרואנציה $x^2 = a \bmod p$.

7. הראו שיש אינסוף פולינומים אי-פריקים בחוג הפולינומים **Z**/3**Z**[x] .

בהצלחה !