תורת המספרים (89256)
תרגיל 2

1. יהי $p>3$ מספר ראשוני. הוכח כי

$$\left(\frac{3}{p}\right)=\begin{cases}1 & : p\equiv 1,11 \bmod 12\\ -1 & : p\equiv 5,7 \bmod 12\end{cases} \tag{1}$$

$$\left(\frac{-3}{p}\right)=\begin{cases}1 & : p\equiv 1 \bmod 6\\ -1 & : p\equiv -1 \bmod 6.\end{cases} \tag{2}$$

2. יהי $p\notin\{2,5\}$ מספר ראשוני. הוכח כי

$$\left(\frac{5}{p}\right)=\begin{cases}1 & : p\equiv 1,4 \bmod 5\\ -1 & : p\equiv 2,3 \bmod 5.\end{cases}$$

3. מצא את המספרים הראשוניים p עבורם קיים פתרון לשקילות

$$x^2+14x+79\equiv 0 \bmod p.$$

4. (א) מצא את הסימן $\left(\frac{-2}{p}\right)$ לכל ראשוני p.

   (ב) יהי $N_k=(p_1p_2\cdots p_k)^2+2$, כאשר p_i הינו הראשוני האי־זוגי ה־i־י. כלומר, $p_1=3, p_2=5, p_3=7, p_4=11$ ...
   יהי q גורם ראשוני של N_k. הוכח כי $q\equiv 1 \bmod 8$ או $q\equiv 3 \bmod 8$.

   (ג) הוכח שיש אינסוף מספרים ראשוניים ששקולים ל־3 מודולו 8.

5. יהי n מספר טבעי, ויהי p גורם ראשוני של n^4-n^2+1. הוכח כי $p\equiv 1 \bmod 12$.

   רמז: הוכח כי -1 ו־3 שניהם שאריות ריבועיות מודולו p.

6. יהי p מספר ראשוני. הוכח כי $7p+3^p-4$ אינו ריבוע.

   רמז: היעזר במשפט הקטן של פרמה, שנלמד בקורס במבנים אלגבריים:
   אם p ראשוני ואם $(a,p)=1$, אזי $a^{p-1}\equiv 1 \bmod p$.