

## שאלה 2

(א) נניח שכך  $\lceil m/2 \rceil$  הבדיקות הוא שלולית מאבדלת לתיאם שלום זה מזה.  
 נניח שקיימים שלם אינדקסים  $i, j$ , המקיימים  
 $(i^2 = j^2) \bmod m$  ;  $h(k, i) = h(k, j)$   
 $(i^2 - j^2 = 0) \bmod m$   
 $((i-j)(i+j) = 0) \bmod m$

מ הוא מספר ראשוני,  $(i-j=0) \bmod m$  או  $(i+j=0) \bmod m$ .  
 נניח אחר, מהתנאים  $\lceil m/2 \rceil \leq i-j \leq \lceil m/2 \rceil$ ,  $i \neq j$ , נקבע שלם יתכן  
 $(i-j=0) \bmod m$ ;  $i \neq j$ ,  $0 \leq i+j \leq 2\lceil m/2 \rceil = m-1$  מהתנאים, נקבע שלם יתכן  $(i+j=0) \bmod m$ .

הוכחה שכך  $\lceil m/2 \rceil$  הבדיקות הוא שלולית מאבדלת לתיאם שלום; אם יר  
 $\lceil m/2 \rceil$  תאים תבוסים, אחת לבסוף מהבדיקות האם תאבד לתיאם שלום.

(ב) נבחר  $m=5$  ונשתמש באנרגיה  $hash(k) = k \bmod m$   
 נניח לבסוף את המפתחות  $0, 1, 4$ . בהמשך, אם נניח לבסוף  
 את המפתח  $10$ , כך הבדיקות יביאו לתיאם תבוסים בלבד.