שאלה 4

(א) נניח שכל $\lceil m/2 \rceil$ הפונקציות הראשונות מהטבלה מתאימות שונים זה מזה.
יהיו שני מיקומים של אינדקסים i, j, המקיימים $0 \le i, j \le \lfloor m/2 \rfloor$, $i \ne j$, כך ש
$h(k,i) = h(k,j)$; אזי $i^2 = j^2 \pmod m$
$i^2 - j^2 = 0 \pmod m$
$(i-j)(i+j) = 0 \pmod m$

m הוא מספר ראשוני, לכן $m \mid (i-j=0)$ או $m \mid (i+j=0)$.
מכך אחד, מתקיים $-\lfloor m/2 \rfloor \le i-j \le \lfloor m/2 \rfloor$, $i \ne j$, נובע שלא יתכן $m \mid (i-j=0)$; מכך שני, מתקיים $2 \le i+j \le 2\lfloor m/2 \rfloor = m-1$, $i \ne j$ נובע שלא יתכן $m \mid (i+j=0)$.
הוכחנו שכל $\lceil m/2 \rceil$ הפונקציות הראשונות מהטבלה מתאימות שונים; אם כן $\lfloor m/2 \rfloor$ תאים תפוסים, אחת לפחות מהפונקציות הבאות תגביל לתא פנוי.

(ב) נבחר $m=5$ לשרשרת בפונקציית הגיבוב $h(k) = k \bmod m$
נכניס לטבלה את המפתחות 0, 1 ו-4. במשך, אם ננסה להכניס את המפתח 10, כל הפונקציות ישלחו לתאים התפוסים בלבד.