<u>האלגוריתם ההסתברותי של מילר- רבין לבדיקת ראשוניות של מספר גדול N</u>
<u>(לדוגמה כאשר N הוא מספר בן 100 ספרות)</u>

רועי כנעני

* האלגוריתם ההסתברותי המהיר והיעיל של מילר ורבין לבדיקת ראשוניות של מספרים גדולים, מבוסס על משפט פרמה ועל המשפט המתמטי הבא (הוכחה ניתן לקרוא בספר – מבוא לאלגוריתמים מאת קורמן לייזרסון וריבסט, כרך ב', עמודים 403, 416):

<u>משפט 33.38:</u>
אם N
Nהוא מספר אי-זוגי פריק, אזי מספר העדים לפריקותו של
הוא לפחות (N - 1) / 2 .

במילים אחרות – עבור N אי זוגי פריק, אם נבחר באופן אקראי מספר K בטווח
N . . 2 = K – 1
לפחות N/2 מספרים מקיימים את התכונה: " K הוא עד לפריקותו של N "
וניתן לחשב (בקלות יחסית) פונקציה המוגדרת בצורה הבאה:

N פריק בוודאות	{ (1) true	Witness(N , K) =
K אינו מעיד אם N פריק או לא	{ false	

<u>האלגוריתם של מילר- רבין לבדיקת ראשוניות של N (אי זוגי)</u>
בצע בלולאה s = 100 פעמים :
א) הגרל מספר שלם K בטווח N . . 2 = K–1

ב) אם

Witness(N , K) =	(1) true

עצור והכרז " N פריק בוודאות " (N אינו מספר ראשוני)
אחרת –
חזור ל א) והגרל מספר K אקראי נוסף.

אם הלולאה הסתיימה ולא נמצא ש N פריק, אזי N הוא ראשוני בהסתברות
$1 - 1/2^{100}$

<u>הסבר:</u>
עבור הגרלת ה K הראשון אם לא הוכרז ש N פריק אז ההסתברות ש N פריק היא P < ½
(כי הגרלנו את K מתוך N/2 עדים לפריקות!).
אחרי שהוגרלו 2 Kים אם לא הוכרז ש N פריק אז ההסתברות ש N פריק היא P < ¼
ואחרי שהוגרלו 100 Kים אם לא הוכרז ש N פריק אז ההסתברות ש N פריק היא
$P(\text{N פריק}) < 1/2^{100}$ => N ראשוני באופן מעשי (למרות שלא הוכח מתמטית)