אלגוריתם של Miller ובדיקת ראשוניות

נתון: מספר טבעי נפוץ n.

(1) בוחרים $1<a\le n-1$ באקראי.

(2) אם $\gcd(a,n)>1$, החזר פריק.

(3) אחרת בדוק האם $a^{n-1}\equiv 1 \pmod n$? אם לא - החזר פריק

(4) אם כן - החזר "כנראה שי-פריק"

*הערה: כיצד מחשב את $a^{n-1} \pmod n$ ביעילות גבוהה, תמיד נשאיר עלי-שורש בתחום

$n-1 \dots 0$ כך שאת הפעולה ביניים בתרגיל הוא חזרה מהתחום, כ"ו נקבע

$m \not\equiv 0 \pmod n$, שעבור $y \pmod n$ $m = m'$.

למה: אם קיים $1<a\le n-1$ כך ש $a^{n-1} \not\equiv 1 \pmod n$ (כ"ו a הוא העדות לכך

ש-n אינו ראשוני) אז לפחות $\frac{n-1}{2}$ מספרים כאלה.

הוכחה: תהי:

$$H = \{ a : 1\le a\le n-1 \quad a^{n-1} \equiv 1 \pmod n \}$$

אזי H היא תת-חבורה של $G = \mathbb{Z}_n^*$, כי ברור ש-H סגורה לכפל.

יתרה מזאת, שעבור $a,b \in H$ מתקיים

$$(ab)^{n-1} = a^{n-1} \cdot b^{n-1} = 1 \cdot 1 = 1 \pmod n$$

לכן $ab \in H$.

לפי משפט Lagrange $|H| \mid |G|$ (הגודל של H מחלק את הגודל של G)

יתר שזה לגודל של G).

יתרה מזאת קיים $a \in G \setminus H$, לכן $|H| \le \frac{|G|}{2}$ (כי הוא מחלק את הגודל של G

$$|H| \le \frac{|G|}{2} \le \frac{n-1}{2}$$

מסקנה: לכן הקבוצה ה-ב"פ כך ש $a^{n-1} \not\equiv 1 \pmod n$, גדולה לפחות

$$(n-1) - |H| \ge \frac{n-1}{2}$$

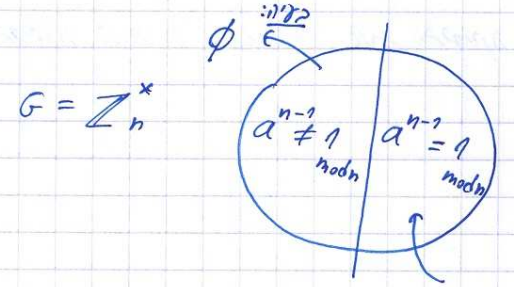
$\blacksquare$

מזה נובע ש הוא כך ש: אם n ראשוני אזי קיים $1<a<n-1$ עבורו $a^{n-1} \not\equiv 1 \pmod n$

אזי בהינתן אחת של האלגוריתם שתיארנו, אם n הוא פריק - נקבל שאר סיכוי $\ge \frac{1}{2}$

אם נחזור t פעמים באופן בלתי תלוי על הוא פריק,

אם n הוא מרוכב נקבל טעות $\leq 1-\left(\frac{1}{2}\right)^t$



נסיק: t פעמים בחירת a שעבורם $a^{n-1} = 1 \pmod n$ הוא בהסתברות $\left(\frac{1}{2}\right)^t$.

הערה ("אפשרות"): קיימים מספרים פריקים n שעבורם $1 < a \leq n-1$ כך ש $a^{n-1} \neq 1 \pmod n$. המספרים הללו נקראים מספרי Carmichael ונדירים.

למה: אם קיים שורש שאינו טריוויאלי למשוואה $x^2 - 1 = 0 \pmod n$ אז n אינו ראשוני.
(כאשר יש תמיד 2 שורשים טריוויאליים $x = 1, -1$).

הוכחה: (א) אם n ראשוני אז $\mathbb{Z}_n$ הוא שדה, ולכן למשוואה ריבועית $x^2 - 1 = 0$ יש לכל היותר שני שורשים בשדה $\mathbb{Z}_n$.

(ב) $n \mid (x-1)(x+1) \iff x^2 - 1 = 0 \pmod n$ (קיבוץ אחרון)
אם n ראשוני אז הוא מתלק או את $(x-1)$ או את $(x+1)$, כ"ז $x = 1 \pmod n$ או $x = -1 \pmod n$ ■

נראה עכשיו את האלגוריתם הקובע בפועל: (בלי להסתבך את כל מס' Carmichael)
נתון: מספר טבעי שקל n.

(1) בודקים $1 < a \leq n-1$ באקראי.

(2) אם $1 < \gcd(a,n)$ התנה פריק.

(3) נרשום $n-1 = 2^k \cdot u$ (u אי-זוגי) שלוקח כ-2 פעולות בלבד.

(4) נחשב $a^{n-1} \pmod n$ באופן הבא: נחשב קודם $b = a^u \pmod n$

ואז נחשב $b^2, b^4, \ldots, b^{2k} = a^{n-1} \pmod n$

(5) נשווה הכל $a^{n-1} = 1 \pmod n$

(6) נתבונן בסדרה: $b, b^2, \ldots, b^{2^{k-1}}, b^{2^k} = 1 \pmod n$,

כאשר נעבור שלב מוסיף (b^{2^k}) שלושלה (6). נבדוק את הבקיקה הבאה:
הסכם האחרון הוא 1 ובקבוק הסכם הקודם לו הוא 1 או 1-.

9/9/05 לית בכרך תשסה

אלגוריתם לחישוב מרחק בין שני מספרים. אלגוריתם הקלט הוא 1- מערך ומחזיר במערכה השלמה.

אלגוריתם הקלט השני הוא 2 משתנה אחד השלמה אורך.