מבחן הראשוניות של מילר - רבין

הערה - משפט וילסון הוא אמ"מ, כלומר, אם p הוא ראשוני אז $(p-1)! \equiv -1 \pmod p$

מהטענה נובעת הדרך הנאיבית: נניח $m>4$, m זוגי, אז $m-1 = 2^1 \cdot s$ כאשר s אי זוגי

↓ הטענת שורש של משפט וילסון: אם p הוא ראשוני אז $x^2 \equiv 1 \pmod p$
עבור $x \in \mathbb{Z}_p$ אז $x \equiv \pm 1 \pmod p$

נניח $g \in \{1,\dots,m-1\}$ נסתכל על $g^{m-1} = g^{2^1 \cdot s} = g^{2^0 \cdot s}, g^{2^1 \cdot s}, g^{2^2 \cdot s}, g^{2^3 \cdot s} \dots g^{2^{k-1} \cdot s}$

ממשפט פרמה הקטן, אם m ראשוני, $g^{m-1} \equiv 1$

נניח ש- $g^{2^{i+1} \cdot s} \equiv 1 \pmod m$, $g^{2^i \cdot s} \not\equiv 1 \pmod m$

נסמן $x = g^{2^i \cdot s}$. קיבלנו $x^2 \equiv 1 \pmod m$, $x \not\equiv 1 \pmod m$ ← $x \equiv -1 \pmod m$

נכונות אלגוריתם שנבנה ממבחן מילר-רבין

בהינתן $m>2$ זוגי, נרשום $m-1 = 2^1 \cdot s$, s אי זוגי
נבחר $g \in \{1,\dots,m-1\}$. נבדוק את הפעולות הבאות:

א) אם $g^{m-1} \not\equiv 1 \pmod m$ פוסלים "m נכשל לפי בסיס g" ועוצרים

ב) אם $g^s \equiv 1 \pmod m$ פוסלים "m עבר לפי בסיס g" ועוצרים

ג) מוצאים את ה-i היחיד המקיים $g^{2^i \cdot s} \not\equiv 1 \pmod m$, $g^{2^{i+1} \cdot s} \equiv 1$
אם $x \equiv -1$ פוסלים "m עבר לפי בסיס g" ועוצרים.
אחרת פוסלים "m נכשל לפי בסיס g" ועוצרים.

* במקרים א', ב', אם m נכשל לפי בסיס g, נקרא "g עד"

משפט - אם m ראשוני, אזי לכל g, האלגוריתם יסתיים בפסלו m "m עבר לפי בסיס g", במילים אחרות לא יהיו עדים לכך ש-m ראשוני.

הוכחנו בעבר למעלה, כמסקנה ממשפט פרמה הקטן והטענה.

משפט - אם m לא ראשוני, אזי

$$|\{g \in \mathbb{Z}_m^* \mid \text{"}m \text{ עבר..."}\}| \le \frac{1}{4}\phi(m) = \frac{1}{4}|\mathbb{Z}_m^*|$$

שימוש במבחן מילר - רבין

בהינתן m "מועמד" שרוצים לבדוק שהוא/ ראשוני. בוחרים k שלמים להיות עדים וסופרים. מבצעים את המבחן עבור m ו-g. אומ בעזרת המקרים m לפן עבר לפי g, אזי בוחרים את m לעבר הראשוני.
אם בלפ אחד מהמקרים m עבר, מסיקים שזה הסתברות ש-m לא ראשוני קטנה מ- $\frac{1}{4^k}$

הערה - עבור g נתון+m נתון, מספר הפעולות החישוביות הנדרשות לביצוע מבחן מילר תין חסום ע"י $O(\log(m))$ שיעורים קבועים c,d.
חסם זמנים זה נקרא "חסם פולי-לוגריתמי" על מספר הפעולות ומעיד על כך שזו בעיה שאפשר לפתור ביעילות במחשבות מחשב.
הבעיה הכללית ביותר במבחן הינו הפלוגה בחלקה (מודולו m) למעט בדיקת g^{m-1} או g^s
אם $m \in S$ מקשה) אופטר לרשום $\mathbb{Z}_m^* \supset I$, $I = \{1,2,3,\dots\}$, $|I| = S$
(פיתוח לפי בסיס 2) למשל: $I = \{1,3,5,7,9,11,13,15\}$, $S = 8$

$$g^s = \prod_{i \in I} g^{2^i} \qquad s = \sum_{i \in I} 2^i$$

מחשבים את $g^{2^{i+1}} = (g^{2^i})^2$ וכך

משפט 2

אם m לא ראשוני, אז $|\{1<m' \le m \mid m' \text{ זר ל-} m\}| \ge \frac{1}{2}\phi(m)$

נוכיח משפט משפט תלת יותר:

משפט 2':

אם m בצורה 2 או 4 או p^k או $2p^k$ עבור ראשוני p, אז

$$|\{1<m' \le m \mid m' \text{ זר ל-} m\}| = \frac{1}{2}\phi(m)$$

הוכחה

נוכיח במקרה פרט של משפט השאריות הסיני:

נניח $\gcd(s,t)=1$, s,t זרים, אז לכל $a_1,a_2 \in \mathbb{Z}$ יש $x \in \mathbb{Z}$

כך ש- $x \equiv a_1 \pmod{s}$, $x = a_2 \pmod{t}$

טענת עזר - נניח ש- m בצורה שלא תלוקה פי ראשוני יותר מ-1.

יהי $M \ge 3$, ונגדיר $S = \{x \in \mathbb{Z}_m \mid \exists j \; x^j \equiv 1 \pmod{m}\}$, ועבור x_0 קטן- $1 \equiv x_0^j$

אזי:

א) $\mathbb{Z}_m^* \ge S$

ב) אם $x,y \in S$ אז $xy \in S$, $x^{-1} \in S$

ג) $|S| \ge \frac{1}{2}\phi(m)$

הוכחת טענת העזר חלק ה':

$x \in S$, אזי $x^j \equiv 1 \pmod{m}$ אז $x^{-j} \equiv x \pmod{m}$

ולכן x^{-j} הפכי של x (מודולו m) כלומר $x \in \mathbb{Z}_m^*$

באופן דומה, אזי $x^j \equiv -1 \pmod{m}$ אז x^{-j} הוא הפכי של x.

ב) נניח $x,y \in S$, $1 \equiv x^j$, $1 \equiv y^i$

$$1 \equiv (1)(1) \equiv y^i x^j \equiv (xy)^{ij}$$

נסמן ב- x הפכי של x, אז $1 \equiv (1) \equiv (x^j)^{-} \equiv (x^{-})^j$

ג) נעזרת $m = s \cdot t$, $s,t \ge 3$ זר"ש, $\gcd(s,t)=1$

יהי $y \in \mathbb{Z}$ כך ש- $y \equiv 1 \pmod{t}$, $y \equiv x_0 \pmod{s}$

(אפשר לפתור ממשפט השאריות הסיני)

כך ש- $y \in S$,

$$y^j \equiv 1^j \equiv 1 \pmod{t}$$

$$y^j \equiv x_0^j \equiv -1 \pmod{s}$$

$$(x_0^j \equiv -1 \pmod{m} \longrightarrow x_0^j \equiv -1 \pmod{s})$$

$$y^j \equiv x_0^j \equiv -1 \pmod{s}$$

אבל $y^j \not\equiv \pm 1 \pmod{m}$ $\leftarrow$ $y \notin S$.

$y \in \mathbb{Z}_m$, כי אם $\gcd(y,m)=d$ אזי ש ראשוני שמחלק את d, ומחלק את s או t

y לא הפך מודולו s או t, סתירה לכך ש- $y^j \equiv 1 \pmod{s}$, $y^j \equiv -1 \pmod{s}$

נסמן $\psi: \mathbb{Z}_m^* \to \mathbb{Z}_m^*$ ע"י $\psi(x) = xy$,

צ"ל הטענה הפיכה, כי אם נגדיר $\theta(x) = xy^{-1}$ אז θ ההפכי של ψ

אם $x \in S$ אז $\psi(x) \in S$ כי אם $\psi(x) = xy \in S$ אז $x = (xy)y^{-1} \in S$
↓ לפי ב'

אז

$$\begin{array}{ccc} \mathbb{Z}_m^* & \xrightarrow{\psi} & \mathbb{Z}_m^* \\ \cup & & \\ S & \to & S \end{array}$$

אז $|S| = |\psi(S)| \leq |S \to \mathbb{Z}_m^*| = |S| - |\mathbb{Z}_m^*|$

הוכחת משפט 2

עבור $x \in \mathbb{Z}_m$ שמן ה- j את הסכום המקסימלי מהצורה $2^s \cdot j$ כך ש- $x^j \equiv -1 \pmod{m}$ (מובטח היטב כי $-1 = (-1)^s$), נסמן $2^s \cdot j = S$ הסכום כנ"ל בהגדרת j, נגדיר את הקבוצה S המופיעה בטענת העזר. נבחר y שבוודאי $\in \mathbb{Z}_m^*$ (כלומר, מהטן מ"ע - רבין בשפ' פס' 6) ש"ך ל- S, ונה יסיים את ההוכחה.