מבחן הראשוניות של מילר - רבין

הערה - משפט וילסון הוא אמ"מ, כלומר, אם p לא ראשוני אז $(p-1)! \not\equiv -1 \pmod p$

מהטענה נובעת העובדה: נניח $m \in \mathbb{N}$. $m \geq 3$, אי זוגי ו $m-1 = 2^{\lambda} \cdot s$

s אי זוגי

הטענה עזר של משפט וילסון: אם p ראשוני ו- $x^2 \equiv 1 \pmod p$

עבור $x \in \mathbb{Z}_p$ אז $x \equiv \pm 1 \pmod p$

נניח $b \in \{1, 2, \ldots m-1\}$ נסתכל על $b^s, b^{2s}, b^{4s}, b^{8s} \ldots b^{2^{\lambda} \cdot s} = b^{m-1}$

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

נניח ש- $b^{2^{r+1}s} \equiv 1 \pmod m$, $b^{2^r s} \not\equiv 1 \pmod m$

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

נכתוב אלגוריתם שנקרא מבחן מילר-רבין

בהינתן $m \geq 3$ אי זוגי, נרשום $m-1 = 2^{\lambda} s$, s אי זוגי

נבחר $b \in \{1, \ldots, m-1\}$. נבצע את הפעולות הבאות:

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

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

ג) מוצאים את ה- r היחיד המקיים $b^{2^{r+1}s} \equiv 1$, $x = b^{2^r s} \not\equiv 1 \pmod m$

אם $x \equiv -1$ פולטים "m עבר לפי בסיס b" ועוצרים.

אחרת פולטים "m נכשל לפי בסיס b" ועוצרים.

* במקרים א, ג, אם m נכשל לפי בסיס b, b נקרא "עד".

משפט 1 - אם m ראשוני, אז לכל b האלגוריתם יסתיים בפלט "m עבר לפי בסיס b", במילים אחרות לא יהיו עדים לכך ש-m לא ראשוני.

הוכחה: נובעת מלמעלה, כמסקנה ממשפט פרמה הקטן והטענה.

משפט 2 - אם m לא ראשוני, אז

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

שימוש במבחן מילר - רבין

בהינתן m "מועמד" שרוצים לבדוק שהוא ראשוני. בוחרים k שלמים להיות עדים פוטנציאליים. מבצעים את המבחן עבור m ו-b. אם באחד המקרים m לא עובר לפי לו אז בודאות m לא ראשוני.

אם בכל אחד מהמקרים m עבר, מסיקים שה הסתברות ש-m לא ראשוני קטנה מ- $\frac{1}{4^k}$

הערה - עבור b נתון ו-m נתון מספר הפעולות החישוביות הדרושות לביצוע מבחן מילר הין חסום ע"י $C(\log(m))^d$ כאשר c, d קבועים.

חסם מסוג זה נקרא "חסם פולי-לוגריתמי" על מספר הפעולות ומעיד על כך שזו בעיה שאפשר לפתור ביעילות באמצעות מחשב.

הבעיה הבעייתית ביותר במבחן היא העלאה בחזקה (מודולו m), למשל בבדיקת b^{m-1} או b^s

אם $s \in \mathbb{N}$ (כלשהו) אפשר לרשום $I \subset \mathbb{Z}_{\geq 0}$, $s = \sum_{i \in I} 2^i$

(פיתוח לפי בסיס 2) למשל: $s = 16$, $I = \{4\}$

$s = 15$, $I = \{0, 1, 2, 3\}$

מחשבים את $b^{2^{i+1}} = (b^{2^i})^2$ ואז $b^s = \prod_{i \in I} b^{2^i}$

Scanned by CamScanner

משפט ב

אם m לא ראשוני. אז $\frac{1}{4}m \geq \frac{1}{4}\phi(m) \geq |\{m \text{ עובר לפי } b \mid b \in \{2,3,\dots,m-1\}\}|$

נוכיח משפט מעט חלש יותר:
משפט ב':
אם $m \geq 3$ אי זוגי ולא חזקה של ראשוני, אז

$$|\{b \in \{2,\dots,m-1\} \mid m \text{ עובר לפי } b\}| \leq \frac{1}{2}\phi(m)$$

<u>הוכחה</u>

ניזכר במקרה פרטי של משפט השאריות הסיני:
נניח $s,t \in \mathbb{N}$, $gcd(s,t)=1$ 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- $m \geq 3$ לא חזקה של ראשוני ואי-זוגי.
יהי $j \in \mathbb{N}$, ונגדיר
$S = \{x \in \mathbb{Z}_m \mid x^j \equiv \pm 1 \pmod{m}\}$, ונניח שקיים x_0 כך ש- $x_0^j \equiv -1$
אזי:
א) $S \subseteq \mathbb{Z}_m^*$
ב) אם $x,y \in S$ אז $xy \in S$, $x^{-1} \in S$
ג) $|S| \leq \frac{1}{2}\phi(m)$

הוכחת טענת העזר א) יהי $x \in S$, אם $x^j \equiv 1 \pmod{m}$ אז $x^{j-1} \cdot x \equiv 1 \pmod{m}$
ולכן x^{j-1} הפכי של x (מודולו m) כלומר $x \in \mathbb{Z}_m^*$
באופן דומה, אם $x^j \equiv -1 \pmod{m}$ אז $-x^{j-1}$ הוא הופכי של x.

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

$$(xy)^j \equiv x^j y^j \equiv (\pm 1)(\pm 1) \equiv \pm 1$$

נסמן ב- x' הופכי של x. אז $(x^{-1})^j \equiv (x^j)^{-1} \equiv (\pm 1)^{-1} \equiv \pm 1$

ג) נרשום $m = s \cdot t$, $s,t \geq 3$ אי זוגיים, $gcd(s,t)=1$

יהי $y \in \mathbb{Z}$ כך ש- $y \equiv 1 \pmod{t}$, $y \equiv x_0 \pmod{s}$
(אפשר לפתור ממשפט השאריות הסיני)

$y \notin S$, כי

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

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

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

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

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

$y \in \mathbb{Z}_m$, כי אם $d = gcd(y,m) > 1$ אז יש ראשוני שמחלק את d, ומחלק את s או t
y לא הפיך מודולו s או t, סתירה לכך ש- $y^j \equiv 1 \pmod{t}$, $y^j \equiv -1 \pmod{s}$

Scanned by CamScanner

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

זו העתקה הפיכה, כי אם נגדיר $\theta(x) = xy^{-1}$ אז θ ההפכי של ψ

אם $x \in S$ אז $\psi(x) \notin S$ כי אם $xy = \psi(x) \in S$ אז $y = (xy)^{-1} x \in S$

↑ לפי ב'

אז $\mathbb{Z}_m^* \xrightarrow{\psi} \mathbb{Z}_m^*$

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

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

הוכחת משפט 2'

נסמן ב- j את המספר המקסימלי מהצורה $j = 2^r s$ עבורו יש $x \in \mathbb{Z}_m$ כך ש- $x^j \equiv -1 \pmod{m}$ (מוגדר היטב כי $(-1)^s \equiv -1$, כלומר $s = s \cdot 2^0$ הוא מספר כזה)
באמצעות j, נגדיר את הקבוצה S המופיעה בטענת העזר.
נראה שכל b שהוא עד (כלומר, מבחן מילר - רבין נכשל לפי b) שייך ל- S, וזה יסיים את ההוכחה.

Scanned by CamScanner