

# תורת 18

## Rabin-Miller בדיקת ראשוניות

$$X_0 \equiv -1 \pmod{n} \iff \begin{cases} X_0^2 \equiv 1 \pmod{n} \\ X_0 \not\equiv 1 \pmod{n} \end{cases}$$

כי: אם  $n$  ראשוני אז  $X^2 \equiv 1 \pmod{n}$  רק עבור  $X \equiv \pm 1 \pmod{n}$ .  
 אם  $n$  אינו ראשוני אז  $X^2 \equiv 1 \pmod{n}$  עבור  $X \not\equiv \pm 1 \pmod{n}$ .

### הוכחה:

יהי  $n$  מס' אי-זכוי זכוי. נרמק:  $n-1 = 2^s t$  אי-זכוי.

יהי  $b \in (\mathbb{Z}/n\mathbb{Z})^*$  הנבחר.

אנו מחפשים  $a_0 = b^t, a_1 = b^{2t}, \dots, a_{s-1} = b^{2^{s-1}t}, a_s = b^{n-1}$  (מחפשים  $n$ ).

אם  $a_0 = \pm 1 \pmod{n}$  - עובר את המבחן עם  $b$  (מנסים  $b$  אחר).

אם  $\exists i, a_i \equiv -1 \pmod{n}$  - אז  $n$  עובר את המבחן עם  $b$ .

אם  $a_i \not\equiv \pm 1 \pmod{n}$  ו- $a_i^2 \equiv a_{i+1} \pmod{n}$  אז  $n$  אינו עובר את המבחן.

אם  $a_s \not\equiv 1 \pmod{n}$  אז  $n$  אינו ראשוני. נחשב  $\gcd(a_s, n)$ .

אם  $a_s \equiv 1 \pmod{n}$  או  $a_j = a_{ord_n b} \equiv 1 \pmod{n}$ , אז  $a_{j-1} = a_j \equiv 1 \pmod{n}$ .

אם  $a_{j-1} \equiv -1 \pmod{n}$  אז  $n$  עובר את המבחן.

אם  $a_{j-1} \not\equiv \pm 1 \pmod{n}$  אז  $n$  אינו עובר את המבחן.

דוגמה: ל- $n=17$  נבחר  $a=2$  ונבדוק.

הוכחה:

(1)  $n=17, e=1$ . אז  $n-1=16=2^4$ .  
 $a_0 = 2^{16} \equiv 1 \pmod{17}$ .

(2)  $n=17, e=4$ . אז  $n-1=16=2^4$ .  
 $a_0 = 2^{4} \equiv 16 \equiv -1 \pmod{17}$ .

אם  $n$  ראשוני  $\begin{cases} b \equiv -1 \pmod{n} \\ b \equiv 1 \pmod{n} \end{cases}$  ו- $a_i \equiv \pm 1 \pmod{n}$ .

$1 = \gcd(n, a_i)$

הוכחה

$$a_0 \equiv b^t \equiv 1^t \equiv 1 \pmod{p^e}, \quad a_0 = b^t \equiv (-1)^t \equiv -1 \pmod{p^e}$$

כל  $n$ ,  $a_0 \not\equiv \pm 1 \pmod{n}$

$$\left. \begin{aligned} a_0 \equiv 1 \pmod{n} &\Rightarrow a_0 \equiv 1 \pmod{p^e} \text{ כל } \left(\frac{k}{p^e}\right) \\ a_0 \equiv -1 \pmod{n} &\Rightarrow a_0 \equiv -1 \pmod{p^e} \text{ כל } \left(\frac{k}{p^e}\right) \end{aligned} \right\} \begin{array}{l} \text{ש.ת.פ} \\ \text{כל מתק"ן } p^e \end{array}$$

$$a_1 = a_0^2 \equiv 1 \pmod{p^e} \Rightarrow a_1 \equiv 1 \pmod{n}$$

$$a_1 \equiv 1 \pmod{p^e}$$

אם  $a_0 \not\equiv \pm 1 \pmod{n}$  אז  $n$  (יש להסתכן)

סעיף 2.1 (הכרחי): אם  $n$  אינו כוזב מורכב אז הוא זרש הסתכן רסין

מיני עקוב, וזכר  $n-b$ .

עקוב  $\triangle$   $10 < a.5 < n$ , יש רק טע' מורכב אחד ספקר את ארבעת הספחים

$b = 2, 3, 5, 7$  (3215031751)

אם הספרת רטון התוספת (Generalized Riemann Hypstheris) נכונה, אז  $b$   $n$  מורכב אי כוזב יש זפריות עם  $b$  אחז ק יש  $a < 2(\log n)^2$ .

$\triangle$  מצאו הדיקת טוילונות בזמן פולינומילי  $\rightarrow$  אבס. Saxena, Kayal, Agrawal

# המשך תוחם 18

## נקודות רציונליות נאיביות

$$\begin{aligned} 0^2+0^2=0^2 & \quad - \quad x,y,z \in \mathbb{Z} & \quad x^2+y^2=z^2 \\ 3^2+4^2=5^2 & & \end{aligned}$$

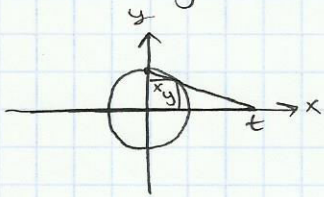
עבור  $z \neq 0$  :  $x = \frac{x}{z}$  ,  $y = \frac{y}{z}$  , אזי  $x^2+y^2=1$  עו מעטל ה' ח' ז' ה'.

נאמר  $(x,y)$  - רציונליות אם  $x,y \in \mathbb{Q}$

כיצד מציבים את כל הנק' הרציונליות ← (המחזוריתם עוקב צל) עקוק ממעלה 2

(1) נבחר נקודה רציונלית על העקוק (נניח שהיא קיימת). למשל  $(0,1)$

(2) נבחר קו ישר רציונלי -  $ax+by=c$  ,  $a,b,c \in \mathbb{Q}$  . נבחר  $y=0$



נעשה הטצה מהנקודה על הישר.

$(x,y)$  - החיתוך של ההטצה עם העקוק.

$$t = \frac{x}{1-y} \quad \text{כיוון,} \quad \frac{t}{1} = \frac{x}{1-y} \quad , \quad (x,y) \rightarrow t$$

אם  $x,y \in \mathbb{Q}$  אזי  $t \in \mathbb{Q}$  . (ראה צד ההפוך)

$$(1-y)^2 t^2 + y^2 = 1 \quad \Leftrightarrow \quad \begin{cases} x = (1-y)t \\ x^2 + y^2 = 1 \end{cases} \quad \Leftrightarrow \quad t = \frac{x}{1-y} \quad t \rightarrow (x,y)$$

$$\begin{aligned} t^2 - 2yt^2 + y^2 t^2 + y^2 &= 1 \\ (t^2+1)y^2 - 2t^2 y + t^2 - 1 &= 0 \\ y^2 - \frac{2t^2}{t^2+1} y + \frac{t^2-1}{t^2+1} &= 0 \end{aligned}$$

פתרון נוסף יוקיים משטות ויטה  $y=1$  פתרון.

$$\begin{aligned} 1+y' &= \frac{2t^2}{t^2+1} \Rightarrow y' \in \mathbb{Q} & \quad x = (1-y)t = \frac{2t}{t^2+1} \in \mathbb{Q} \\ 1 \cdot y' &= \frac{t^2-1}{t^2+1} \end{aligned}$$

$$y = \frac{t^2-1}{t^2+1} , \quad x = \frac{2t}{t^2+1} \quad \text{כיוון,} \quad t \in \mathbb{Q} \Leftrightarrow x,y \in \mathbb{Q}$$

זכור התשטנה: כל הנק' הרציונליות על העקוק  $x^2+y^2=1$  הן  $(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1})$  ,  $t \in \mathbb{Q}$

(0,1) פתל

$$\frac{t^2-1}{t^2+1} = \frac{u^2-v^2}{u^2+v^2} ; \quad \frac{2t}{t^2+1} = \frac{2uv}{u^2+v^2} \quad \text{אם נרשום} \quad t = \frac{u}{v} \quad , \quad u,v \in \mathbb{Q}$$

$$x^2+y^2=z^2 \quad \text{כאן} \quad x=2uv \quad , \quad y=u^2-v^2 \quad , \quad z=u^2+v^2$$

$$x,y,z \in \mathbb{Z}$$