

מבחני ראשוניות

הזר מחמם ים בהזדמיות כמו אחריו שם קרבו, ע"כ
מקובל ש'א' עממו את המושגים חסידות $\varphi = p-1$ כאשר p ים
(ראשוניים מאורגנים (100 סדרה) כיצד נמצא ראשוני מאורגן (100 סדרה).
כיצד נמצא ראשוני מאורגן?

ה'יוני' כמות ה'ראשוניים' ע'ס' א'ט' ג' ה'יא' ג'ר' (100)
מ'ס' ה'ראשוניים'.

$$\frac{x}{\log x} \approx |\{p \leq x\}|$$

ע'כ' נ'ר' א'ח'י'ז' כ'י'ן' ר'ג' א' ה'ס'י'כ'ו' ש'י'ב'י' ראשוני ה'יא' ב'ר' ה' (100)
ה'יוני' כיצד נקרא ה'מ'ס' ר'ת'ן' (א'ו' ש'ה'ל' א'ר'ו' ראשוני' ג'ע'מ'ת'?
מ'ס'ת' ה'ש'ל'ל' ע'י'ת'י'ם' י'ס'ל'י'ם' ל'ש'ל'ת' ג'י'ת' ע'ל'א' א'מ'נ'א' ס'י'כ'ו'ק' ל'ראשוני'ם'
ז'י'ב' ע'ל'.

$$\frac{1}{p} \equiv 1 \pmod{p-1} \Leftrightarrow p \text{ ראשוני} \rightarrow \text{לא יע'ל'}$$

מ'בח'ן' כ'מ'ת'י' א'ט' ה' ראשוני' ו' א'ט' כ'ט' א'ס' (ה'מ'ס'ל' $a^{n-1} \equiv 1 \pmod{n}$)
כ'ר' - (ה'מ'ס'ל' $a^{n-1} \not\equiv 1 \pmod{n}$) א'ס' ה'ל'א' ראשוני'.

א'ט'ו' כ'י'ס' מ'ת'א'י'ם'.
נ'ק'ר'ע' מ'ר'א'ש' כ'מ'ל'ת' א'י' (ז'י'ת' ו').
נ'ב'צ'ע' י'ס'מ'י'ם'.
נ'ר'י'ל' מ'ס' $1 \leq a \leq n-1$
נ'ב'ד'ו'ק' ה'כ'א'ס' (ה'מ'ס'ל' $a^{n-1} \equiv 1 \pmod{n}$) (א')
א'י' כ'ד'ו'ק' ה'י' א'ט' א'ט' מ'ק'י'ט' א'ט' (א') א'ס' ה'ל'א' ראשוני'.

ה'ב'ד'ר'ת' א' נ'ק'ר'ע' כ'מ'ל'ת' ראשוני' א'ו'כ'א'י' מ'ז'ו'מ'י' (Pseudo Prime) ל'כ'י' ג'ס'ס' א' א'ט'.
 $a^{n-1} \equiv 1 \pmod{n}$

ס'י'כ'ו' ה'ל'מ'ת' ה'א'ט'ו'ל'ק' מ'א'י' (ז'י'ת' ו') א'ח'ר' ה'וא' א'ח'ל'ס' י'ת'ע'ס'ס' א'ט' ג'מ'י'ח'ס' א'ד'י'ת'ס' ה'
א'י'ו' ס'ס'א'ב'ו' - ראשוני'.

(ס'ט'ר'ת' ה'י'מ'י'ס' מ'ס' ה' א'י'נ'ק' ראשוני' כ'ר' ל'ט' א'ט' כ'ט' א'ס' (ה'מ'ס'ל' $a^{n-1} \equiv 1 \pmod{n}$).

מ'ס'ט'ר'י'ם' א'י' ה'נ'ק'ר'ע' א'ט' ס'ס'כ'י' ה'ו'מ'י'ק'ל' (Carmichael)

$$a^{560} \equiv 1 \pmod{560} \quad \forall a \quad n=560=2^3 \cdot 7 \cdot 5$$

$$a^{560} \equiv 1 \pmod{2^3} \pmod{7} \pmod{5}$$

$$a^{560} = (a^8)^{70} \equiv 1^{70} \equiv 1 \pmod{3}$$

$\beta \leq p_{n-k}$ (ע"פ), $h = p_{n-k} \cdot p_k$ β^k קומ"ח, β^k (נ"א מ"ש) β^k ונ"ח כ' β^k (נ"א מ"ש) β^k ונ"ח כ' β^k (נ"א מ"ש) β^k ונ"ח כ' β^k (נ"א מ"ש)

ה'רמק! יצא ד' מ'סוקצ' ק'רמ'ק' ש'ס'ר'ו ה'ג'ת.

$$\pi(2^j) = \begin{cases} 1 & j=1 \\ 2 & j=2 \\ 2^{j-2} & j \geq 3 \end{cases}$$

$$K = \{ p_1^{j_1} p_2^{j_2} \dots p_n^{j_n} \mid j_i \geq 0, i=1, \dots, n \}$$

$$a^{b-1} \equiv 1 \pmod{b} \Rightarrow \text{ord}_b(a) \mid b-1$$

$$\text{ord}_b(a) \mid \lambda(b)$$

$$SIC, \left(d, \overbrace{d', d, \dots, d}^{\max\{d, n, n/2\}}, 0, n \right)_{n-d, 5a}$$

SR, $p_1, p_2, p_3, \dots, p_n$, $h = p_1^{j_1} \dots p_n^{j_n}$ p. 17

$$P_i = L_{p_i} \cdot \frac{1}{h} \quad \text{and} \quad \int_{\mathbb{R}^n} P_i \, d\lambda = 1 \quad \text{for} \quad i = 1, 2, \dots, n$$

176, 1729, 10585 176, 1729, 10585

הקבוצה $\{a^{n/2^k} \pmod n\}$ היא תת-קבוצה של $\{1, -1\}$ ולכן $a^{n/2^k} \pmod n \in \{1, -1\}$

אם $a^{n/2^k} \pmod n = 1$ אז $a^{n/2^{k-1}} \pmod n = \pm 1$

$$\begin{aligned} a^{n/2^k} \pmod n &\equiv 1 \iff a^{n/2^{k-1}} \pmod n \equiv \pm 1 \\ a^{n/2^k} \pmod n &\equiv -1 \iff a^{n/2^{k-1}} \pmod n \equiv \pm i \end{aligned}$$

אם $a^{n/2^k} \pmod n \neq \pm 1$ אז $a^{n/2^k} \pmod n$ הוא מספר מרובע חזק. נניח $a^{n/2^k} \pmod n = x$. אז $x^2 \equiv 1 \pmod n$ ו- $x \not\equiv \pm 1 \pmod n$. לכן x הוא מספר מרובע חזק.

למשל: $n=15$

אם $a=2$, אז $2^{15/2} \pmod{15} = 2^7 \pmod{15} = 8$. אז $8^2 \pmod{15} = 64 \pmod{15} = 4$. אז $4^2 \pmod{15} = 16 \pmod{15} = 1$. לכן 2 הוא מספר מרובע חזק.

אם $a=7$, אז $7^{15/2} \pmod{15} = 7^7 \pmod{15} = 1701 \pmod{15} = 6$. אז $6^2 \pmod{15} = 36 \pmod{15} = 6$. לכן 7 הוא מספר מרובע חזק.

אם $a=11$, אז $11^{15/2} \pmod{15} = 11^7 \pmod{15} = 194871 \pmod{15} = 1$. לכן 11 הוא מספר מרובע חזק.

לכן, אם a הוא מספר מרובע חזק, אז $a^{n/2^k} \pmod n \in \{1, -1\}$. אחרת, $a^{n/2^k} \pmod n$ הוא מספר מרובע חזק.

אם a הוא מספר מרובע חזק, אז $a^{n/2^k} \pmod n \in \{1, -1\}$. אחרת, $a^{n/2^k} \pmod n$ הוא מספר מרובע חזק.

משפט	דוגמה 1: $a=3, n=25$	דוגמה 2: $a=7, n=25$
$2^0 \equiv 1 \pmod{11}$	$3^0 \equiv 1 \pmod{25}$	$7^0 \equiv 1 \pmod{25}$
$2^1 \equiv 2 \pmod{11}$	$3^1 \equiv 3 \pmod{25}$	$7^1 \equiv 7 \pmod{25}$
$2^2 \equiv 4 \pmod{11}$	$3^2 \equiv 9 \pmod{25}$	$7^2 \equiv 49 \equiv -1 \pmod{25}$
$2^3 \equiv 8 \pmod{11}$	$3^3 \equiv 27 \equiv 2 \pmod{25}$	$7^3 \equiv -7 \pmod{25}$
$2^4 \equiv 5 \pmod{11}$	$3^4 \equiv 81 \equiv 6 \pmod{25}$	$7^4 \equiv 1 \pmod{25}$
$2^5 \equiv 10 \pmod{11}$	$3^5 \equiv 243 \equiv 18 \pmod{25}$	$7^5 \equiv 7 \pmod{25}$
$2^6 \equiv 7 \pmod{11}$	$3^6 \equiv 729 \equiv 4 \pmod{25}$	$7^6 \equiv -7 \pmod{25}$
$2^7 \equiv 3 \pmod{11}$	$3^7 \equiv 2187 \equiv 12 \pmod{25}$	$7^7 \equiv 1 \pmod{25}$
$2^8 \equiv 5 \pmod{11}$	$3^8 \equiv 6561 \equiv 6 \pmod{25}$	$7^8 \equiv 7 \pmod{25}$
$2^9 \equiv 10 \pmod{11}$	$3^9 \equiv 19683 \equiv 18 \pmod{25}$	$7^9 \equiv -7 \pmod{25}$
$2^{10} \equiv 7 \pmod{11}$	$3^{10} \equiv 59049 \equiv 4 \pmod{25}$	$7^{10} \equiv 1 \pmod{25}$
$2^{11} \equiv 3 \pmod{11}$	$3^{11} \equiv 177147 \equiv 12 \pmod{25}$	$7^{11} \equiv 7 \pmod{25}$
$2^{12} \equiv 5 \pmod{11}$	$3^{12} \equiv 531441 \equiv 6 \pmod{25}$	$7^{12} \equiv -1 \pmod{25}$
$2^{13} \equiv 10 \pmod{11}$	$3^{13} \equiv 1594323 \equiv 18 \pmod{25}$	$7^{13} \equiv 7 \pmod{25}$
$2^{14} \equiv 7 \pmod{11}$	$3^{14} \equiv 4782969 \equiv 4 \pmod{25}$	$7^{14} \equiv -7 \pmod{25}$
$2^{15} \equiv 3 \pmod{11}$	$3^{15} \equiv 14348907 \equiv 12 \pmod{25}$	$7^{15} \equiv 1 \pmod{25}$