

אומרים לך 13 סופרים בפרק ב. (אם כי יש שכתבו 14).

Q1: 13th July - 3000.

91 י' 13"00 0005 2 ← 91 157 11017

מספרי דרמ"ק פס"ב ראשונים א. ס. ס. .

טענה: א) מ' צוזי איין מ' קרמיקע

(פ) אם ה מתחזק כריבוע אז הוא אינו מט' קרמ"ק

ע) אם n (נסו) ריבועי, אי צדי אן א קרמיקז $\Leftrightarrow$ נאטורל n/p מתק"ס $(n-1) \mid (n-p)$

③ מט' תרמ"ק ה'ה' מרפא' ע' נפשות 3 הושינ"ס.

הוכחה:

ד) $b = -1$ (שיעור קוצר)

פ' יהי א מל' דרמ"ת, ק כאשני או צודי דמחזק את א. ע"ח α/p^2 .

ה' g ש"ל מובן, p^2 כן, $\ell := \text{ord}_p(r)$

נבחר b כך $b \equiv g(p^e)$
 $b \equiv 1 \pmod{n/p^e}$

$$(gcd(\frac{n}{p^e}, b) = 1, gcd(b, p^e) = 1 \Rightarrow gcd(b, n) = 1 \quad \text{if } p \nmid b$$

מכיון ש- h קרובה $b^{n-1} \equiv 1 \pmod{b^n}$ ו- $b^{n-1} \equiv 1 \pmod{b^n}$ כי $b^{n-1} \equiv 1 \pmod{b^n}$, $g^{n-1} \equiv 1 \pmod{b^n}$, $g^{n-1} \equiv 1 \pmod{b^n}$

$$\Leftarrow p|n \Rightarrow p|n-1 \Rightarrow p \mid p(p-1) \mid n-1 \Rightarrow \text{ord}_{p^2} g = \varphi(p^2) = p(p-1)$$

□ פ"א כי מן!

(p) $\begin{cases} b = g(p) \\ b = 1 \text{ (if } p \end{cases}$ - (b) $\boxed{\leftarrow}$

כִּי $b \equiv 1 \pmod{p}$ וְכִי $b \equiv 1 \pmod{q}$.

$\sqrt{p-1 \mid n-1}$ י"כ $g^{n-1} \equiv 1(p)$ י"כ

• n - מס' ב $\mathbb{Z}$ חי' . $\forall i$: $p_i - 1 \mid n_i - 1$, $n = p_1 \cdot \dots \cdot p_r$ $n \nmid 1$ $\Rightarrow$

$$b^{k-1} = (b^{p_i-1})^{m_i} \equiv 1^{m_i} \equiv 1(p_i) \iff k-1 = m_i(p_i-1)$$
$$p_i \nmid b \quad p_i \nmid k \mid b^{k-1} - 1 \quad \text{vs} \quad \forall i \quad p_i \mid b^{k-1} - 1 \quad \text{vs}$$
$$\boxed{\nabla} \quad b^{h-1} \equiv 1(n) \quad \Leftarrow$$

॥ नमो नमो ३

צדקות: $501 = 3 \cdot 11 \cdot 17$, $2|500$, $10|500$, $100|500$

פסיידו ראשוניים של אוילר

יהי n שלם אי צד (חזק). אם a ראשוני מתקיים: $\forall b \in \mathbb{Z}_{n-1}^* \quad b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$

הצדקה: אם a מט אי צד מורכב, ויהי b שלם כך ש $\gcd(b, n) = 1$

אזי אם $\otimes$ מתקיים אומרים ש a פסיידו ראשוני של אוילר בקסם b .

צדקה: 91 פסיידו ראשוני 3-5. האם פסיידו ראשוני סטאוילר 23-5? לא.

⚠️ אין מט שיהא פסיידו ראשוני אוילר על הזרים אזי (נכח).

⚠️ קור שאל מט פסיידו ראשוני אוילר 5-3 $\leftarrow$ פסיידו ראשוני 5-3.

משפט: יהי a מט אי צד מורכב. אז עבור צדקות 50% מתקיים b ,

$$b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod{n} \quad \gcd(b, n) = 1, 1 < b < n$$

מבחן סושוניר סולובאי-סטרסן

a אי צד. נבחר a שלמים b , $1 < b < n$ (נבדוק צדקות).

מהם $\otimes$. אם נאחד מהם לא מתקיים, a אינו ראשוני. אחרת קיבלנו

ש- a לא ראשוני בהסתברות $\geq \frac{1}{2^k}$ (כ- $1 - \frac{1}{2^k}$ הוא ראשוני).

* את שני הודפים מחשבים ב- $O(k^3 \log n)$ - פנימיטאז.

הוכחת המשפט:

למעשה: נניח a מורכב, אזי קיים $b \in \mathbb{Z}_{n-1}^*$, $\gcd(b, n) = 1$ שא מתקיים עבורו.

הוכחה: אם $\exists k$ כך ש $a^k \equiv 1 \pmod{n}$ אז a אינו קרטיק, וכן $\exists k$ כך

$$a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n} \quad \text{והוא צד.}$$

נניח שכן a מופת ראשוני שונים. יהי a ראשוני, $\gcd(a, p) = 1$.

(נבחר b כך ש $\gcd(b, p) = 1$ - (צד p קיים נכח).

משקול: כפירה, קיימים צד שאינן ריבועות של שלמים).

קיים b כך ש $b \equiv a \pmod{p}$ (קיים כי צד, שווה סני).

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p}\right) \cdot \left(\frac{b}{\frac{n}{p}}\right) = \left(\frac{b}{p}\right) \cdot 1 = -1$$

$$b^{\frac{n-1}{2}} \equiv 1 \pmod{n} \Rightarrow b^{\frac{n-1}{2}} \equiv 1 \not\equiv -1 \equiv \left(\frac{b}{n}\right) \pmod{n}$$

כן b הוא צד. $\blacksquare$

תבנית תחום 17

הוכחת המשפט:

יהיו $0 < a_i < n$, $i=1, \dots, k$, שונים וזרים ל- n כך $a_i \equiv a_j \pmod{n}$ נכוח $k \leq \frac{\varphi(n)}{2}$.

קיים b מהצורה $2^s \cdot t$ שאינה מתקיימת עבור n .

נבחר r_i השווה ל- $a_i b$ בחזקת n .

אזי $r_i \neq r_j$ $\forall i \neq j$ כי בחזקת $(\frac{\varphi(n)}{2})^x$ מתקיים חוק צטנר

$$(a_i = a_j \iff a_i b = a_j b)$$

$$r_i \equiv a_i^{\frac{n-1}{2}} \pmod{n} \iff a_i^{\frac{n-1}{2}} b^{\frac{n-1}{2}} \equiv (a_j)^{\frac{n-1}{2}} b^{\frac{n-1}{2}} \pmod{n} \iff (a_i)^{\frac{n-1}{2}} \equiv (a_j)^{\frac{n-1}{2}} \pmod{n} : \forall i, j; a_i \neq r_j$$

ענן r_j עדיף ואכן $a_i \neq r_j$ $\forall i, j$ (כי a אינם עדיפים).

$$|\{a_i\}| + |\{r_j\}| = 2k \leq |(\frac{\varphi(n)}{2})^x|$$

$$\square \quad k \leq \frac{\varphi(n)}{2}$$

מבחן מילר-ראבין Rabin Miller

רמיון: אם n ראשוני, $\chi_0^2 \equiv 1 \pmod{n}$, $\chi_0 \neq 1 \pmod{n}$ אזי $\chi_0 \equiv -1 \pmod{n}$

כי $2 \nmid \frac{\varphi(n)}{2}$ שבה.