## הסדר א איברי ב- $\mathbb{Z}_n^*$ ושורשים פרימיטיביים

ראינו אם $a\in\mathbb{Z}_n^*$, כלומר $a$ זר ל-$n$, אזי $a^{\phi(n)}\equiv 1 \pmod n$

הערה: זה נכון לכל $a$. אם $a$ זר ל-$n$, נגדיר את $\mathrm{ord}_n(a)$ להיות המינימלי $d$ הקטן ש- $a^d\equiv 1 \pmod n$. לפי משפט אוילר, $d\le\phi(n)$.

למה: $n$ טבעי, $a$ זר ל-$n$. אם $a^k\equiv 1 \pmod n$ אז $\mathrm{ord}_n(a)\mid k$. בפרט, $\mathrm{ord}_n(a)\mid\phi(n)$

הוכחה: נחלק עם שארית: $k\equiv L\cdot\mathrm{ord}_n(a)+r$, $0\le r<\mathrm{ord}_n(a)$. אז

$$\underbrace{a^k}_{\equiv 1}=\underbrace{\left(a^{\mathrm{ord}_n(a)}\right)}_{\equiv 1}^{L}\cdot a^r \quad \text{מתקיים}$$

לכן $a^r\equiv 1 \pmod n$. ובגלל ש-$\mathrm{ord}_n(a)$ הוא הטבעי המינימלי שמקיים זאת ו-$0\le r<\mathrm{ord}_n(a)$ נובע ש- $r=0$.

שימו לב שאם $d=\mathrm{ord}_n(a)$

אז $(a^k)^d\equiv 1 \pmod n$ לכל $k\ge 0$, לכן $\mathrm{ord}_n(a^k)\mid\mathrm{ord}_n(a)$

טענה: יהי $n\ge 1$ טבעי, $a$ זר ל-$n$, $m\ge 0$ טבעי. אזי:

$$\mathrm{ord}_n(a^m)=\frac{\mathrm{ord}_n(a)}{\gcd(m,\mathrm{ord}_n(a))}=$$

$(\gcd(a,b)\cdot\mathrm{lcm}(a,b)=a\cdot b)$

$$=\frac{\mathrm{lcm}(\mathrm{ord}_n(a),m)}{m}$$

הוכחה: נסמן $d=\mathrm{ord}_n(a)$, $r=\mathrm{ord}_n(a^m)$.

ידוע כי $(a^m)^r\equiv 1 \pmod n$

לכן $d\mid m\cdot r$. מה ה-$r$ המינימלי שעבורו $d\mid mr$?

נסמן $b=\gcd(d,m)$, ואז $m=bm_1$, $d=b\cdot d_1$, ונקבל ש-

$$d=\underline{\underline{b}}d_1\mid mr=\underline{\underline{b}}m_1r$$

לכן $d_1\mid m_1r$ ומכאן $d_1\mid r$ כיוון ש- $\gcd(d_1,m_1)=1$.

בפרט, $r\ge d_1=\frac{d}{b}$. לסיום, נבדוק!

$$(a^m)^{\frac{d}{b}}=(a^d)^{\frac{m}{b}}\equiv 1^{\overset{\text{טבעי}}{\frac{m}{b}}}\equiv 1 \pmod n$$

לכן: $r=\mathrm{ord}_n(a^m)=\frac{d}{\gcd(d,m)}$ ∎

Scanned by CamScanner

**הגדרה:** יהי n טבעי, a זר ל-n. a הוא <u>שורש פרימיטיבי</u> מודולו n אם: $\text{ord}_n(a)=\phi(n)$

במקרה כזה: $\{a^i \mid 1\le i\le\phi(n)\}\equiv\mathbb{Z}_n^*$

כדי לראות זאת נבחין שאם קיימים $0\le i\le j<\phi(n)$ כך ש- $a^i\equiv a^j \pmod n$ אז כיוון ש-a הפיך, $a^{j-i}\equiv 1 \pmod n$, וכיוון ש- $j,i<\phi(n)$ נקבל ש- $j-i=0$ כי $\text{ord}_n(a)=\phi(n)$

במונחים יותר אלגבריים (חבורות), $\mathbb{Z}_n^*$ היא ציקלית, כלומר שקולה לחבורת $\{0,1,\dots,\phi(n)-1\}$ עם פעולת החיבור מודולו $\phi(n)$ ע"י המיפוי:

$$\begin{tikzcd}
a^m \arrow[r, mapsto] & m \\
\mathbb{Z}_n^* \arrow[u, phantom, sloped, "\in"] & \mathbb{Z}_{\phi(n)} \arrow[u, phantom, sloped, "\in"]
\end{tikzcd}$$

[illegible]

<u>בעיה מעניינת שעולה מרעיונות אלה:</u>

אם ידוע לנו ש-a שורש פרימיטיבי מודולו n ונתון $b\in\mathbb{Z}_n^*$, מצא i כך ש- $a^i\equiv b \pmod n$ (בלוגריתם. למה? נסמן: $i=\log_a(b)$). זו בעיה קשה. לא ידוע לה פתרון יעיל.

[illegible]

**<u>עוד שאלה:</u>** לאילו n יש שורש פרימיטיבי? $\mathbb{Z}_n^*$-ב

(קל מאוד!) ⇐ **<u>שאלה נוספת!</u>** אם ל-n יש שורש פרימיטיבי, כמה שורשים פרימיטיביים כאלה יש לו?

תשובה: $\phi(\phi(n))$, משום שאם a שורש פרימיטיבי אז $a^m$ שורש פרימיטיבי אמ"מ $1=\gcd(\underbrace{\text{ord}_n(a)}_{\phi(n)},m)$.

$$\Downarrow$$

$$1=\gcd(\phi(n),m)$$

**<u>שאלה פתוחה במתמטיקה!</u>**

האם יש אינסוף ראשוניים p עבורם 2 הוא שורש פרימיטיבי? ידוע ש-RGH גורר שכן. ידוע שאחד מ-{2,3,5} הוא שורש פרימיטיבי לאינסוף ראשוניים...

<u>לגבי השאלה השנייה, נוכיח את המשפט הבא:</u>

**<u>משפט:</u>** מודולו n, קיים שורש פרימיטיבי אמ"מ

$n=2$

$n=4$

$n=p^j$, p ראשוני, זוגי

$n=2p^j$, p ראשוני זוגי

V

לא נוכיח רק משמעות מכיוון זה.

למשל נראה שאם $r,s>2$ זרים ו- $n=r\cdot s$ אז לכל a שזר ל-n $a^{\frac{1}{2}\phi(n)}\equiv 1$. כלומר <u>אין</u> שורש פרימיטיבי.

לכן אם בפירוק לראשוניים יש שני ראשוניים $\ge 3$ שונים אז מודולו n אין שורש פרימיטיבי.

Scanned by CamScanner

ר'נגיים, $n=2^a p^b$, $p\geq 3$ ראשוני, $a,b\geq 0$.

כמו כן, אם $a\geq 2$, $b\geq 1$ אז $n=\underbrace{2^a}_{r}\underbrace{p^b}_{s}$ ולכן אין שורש פרימיטיבי.

המקרה היחיד עבורנו אין שורש פרימיטיבי ולא מכוסה ע"י 1+2 טענות אלה. הוא

כמו כן, $a\geq 3$, $n=2^a$ מתקיים זו... (תרגיל בית).

המקרים $n=2$, $n=4$, טריוויאלים. עבור $n=2$ 1 הוא שורש פרימיטיבי.

עבור $n=4$, 3 הוא שורש פרימיטיבי, $\mathbb{Z}_4^*\equiv\{1,3\}\equiv\{3^1,3^2\}$ מודולו 4.

<u>משפט!</u> (מקרה פרטי של הקודם)

אם $p\geq 3$ אז יש שורש פרימיטיבי מודולו $p$......

<u>הוכחה!</u> לכל מחלק $d$ של $p-1$ נגדיר

$$\psi(d)=|\{a\in\mathbb{Z}_p^*: ord_p(a)=d\}|$$

כמו כן, אם $a$ זר ל-$p$ אז $ord_p(a)|\phi(p)=p-1$ מכאן:

$$(*)\quad \sum_{d|p-1}\psi(d)=p-1$$

למדנו בעבר ש-

$$(**)\quad \sum_{d|p-1}\phi(d)=p-1$$

נוכיח ש- $\psi\overset{\text{לכל } d|p-1}{=}\phi$ ונסיים, כי בפרט $1\leq\psi(p-1)=\phi(p-1)$

נוכיח קודם שאם $\psi(d)\neq 0$ אז $\psi(d)=\phi(d)$, ומכאן ינבע השוויון גם כאשר $\phi(d)=0$,

כיוון ש- $(*)$ ו- $(**)$ מתקיים!

$$\sum_{d|p-1}\psi(d)=\sum_{d|p-1}\phi(d)$$

$$\sum_{\substack{d|p-1\\ \psi(d)\neq 0}}\psi(d)+\underbrace{\sum_{\substack{d|p-1\\ \psi(d)=0}}\psi(d)}_{=0}\overset{(\square)}{=}\sum_{\substack{d|(p-1)\\ \psi(d)\neq 0}}$$

$\Downarrow$

ע"י הערכת אגפים כי $\sum_{\substack{d|p-1\\ \psi(d)=0}}\psi(d)=0$, ולכן לכל d כך ש- $\phi(d)\geq 1$ $\psi(d)\neq 0$

נותר להוכיח את (ב)

נניח $d|p-1$. נניח כי $\psi(d)\neq 0$ ויהיה $a$ ו-$p$, כך ש- $ord_p(a)=d$

מהגדרת החזקות א' אחר לזו:

$$a^1, a^2, \dots, a^d$$

מודולו $p$ אלה מס' שונים, כי אם $a^i\equiv a^j \pmod p \Rightarrow i=j$ כפי שהראינו.

(ראינו כי $ord_p a^m=\frac{d}{gcd(m,d)}$

בסה"כ יש לנו בדיוק $\phi(d)$ חזקות רלוונטיות ש- $ord_p(a^m)=d$, ולכן $\psi(d)\leq\phi(d)$

נראה שאם $b^d\equiv 1 \pmod p$ אז $b$ הוא חזקה של $a$ ומכאן נסיים.

הדבר נובע ממשפט לגרנז' - לפולינום $x^d-1$ יש לכל היותר $d$ שורשים מודולו $p$, כל החזקות של $a$ הן שורשים ולכן אלה השורשים היחידים. ∎