תרגול 12

טענה 2: אם $p \neq 2$ אז החבורה $(\mathbb{Z}/p^2\mathbb{Z})^\times$ היא ציקלית (יש שם).

יש שם $g \in \mathbb{Z}$ כך ש- $g^{p-1} \not\equiv 1 \pmod{p^2}$ אז g הוא שם שבור p. זאת הוכחנו. צ"ל שהסדר של g מודולו p הוא $\varphi(p^2)$. מספיק להראות שאם $g^n \equiv 1 \pmod{p^2}$ אז $n \mid \varphi(p^2)$.

נסמן $p^{e-1}(p-1) = \varphi(p^e)$. נסמן $n \mid p^{e-1}(p-1)$. כלומר $n = p^{e-1}\cdot n'$.

אז $g^{n'(p-1)} = g^n$. לפי פרמה $g^{p-1} \equiv 1 \pmod{p}$

נכון $g^{n'} \equiv g \pmod{p}$ $\Leftarrow$ $g = g^{(p-1)\cdots(p-1)} = g^{\varphi(p)\cdots\varphi(p)}$

מכיוון ש- $g^n \equiv 1 \pmod{p^2}$ אז בפרט $g^n \equiv 1 \pmod{p}$

נכון $g^{n'} \equiv g \pmod{p}$. כלומר g הוא שם שבור מודולו p הוא $p-1$.

נכון $p-1 \mid n'$ $\Leftarrow$ $p^{e-1}(p-1) = \varphi(p^e) \mid n$ ונכון g הוא שם שבור p. ∎

דוגמא: $p=3$:

$2 = \varphi(9)$. 2 הוא שם שבור מודולו 3. $2^2 = 4 \not\equiv 1 \pmod{9}$.

נכון 2 הוא שם שבור 3^3 שלא. לעומת שבור $2 \cdot 3^3 = 27$.

נסתכל על: $81 = 3^2 \cdot 3 - 2 = \varphi(27)$ כי $81 = \varphi(27) \mid 2^{81} - 1$ לפי או"ר.

כי $81 \nmid 2^{\varphi(27)/3} - 1$

מספיק לבדוק ש $9 \mid 9$. $2^9 = 512 = 19 \cdot 27 + 19 \equiv 19 \pmod{27}$

נכון 2 אכן שם שבור 27.

$2^9 = 512 = 19 \cdot 27 + 19 \equiv 19 \pmod{27}$

טענה 4: החבורות $(\mathbb{Z}/2\mathbb{Z})^\times$, $(\mathbb{Z}/4\mathbb{Z})^\times$ הן ציקליות.

אם $e \geq 3$ החבורה $(\mathbb{Z}/2^e\mathbb{Z})^\times$ אינה ציקלית.

הסדר של $\bar{5}$ ב- $(\mathbb{Z}/2^e\mathbb{Z})^\times$ הוא 2^{e-2}.

הוכחה: $5^{2^{e-3}} = (1+4)^{2^{e-3}} = 1 + 2^{e-1} + c \cdot 2^e$ כאשר $c = 0$ או 1, ניתנת את כל האברים

$(\mathbb{Z}/3^3\mathbb{Z})^\times$, $\varphi(27) = 18$ (1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26)

משפט: יהי $n = a^{a_0} p_1^{a_1} \cdots p_k^{a_k}$. אז $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/a^{a_0}\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times$

יהי $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ היא חבורה בגודל $\varphi(p_i^{a_i})$.

$(\mathbb{Z}/2\mathbb{Z})^\times$ היא חבורה בת איבר אחד. $(\mathbb{Z}/2^2\mathbb{Z})^\times$ חבורה בגודל 2 איברים.

$(\mathbb{Z}/2^a\mathbb{Z})^\times$ עבור $a \geq 3$ היא חבורה שאינה ציקלית מסדר 2^{a-2} על יוצר $\overline{-1}$-

ותבורה בגודל 2^{a-2} על יוצר $\overline{5}$.

המשפט הזה שימושי לקבוצה:

שאלה: עבור איזה n יש שורש פרימיטיבי? $\varphi(2+d)$, $\varphi(2+d)$, 2, 4

הוכחה: * הוכיחנו φ, 2, 4

* עבור φ: $(\mathbb{Z}/2^d\mathbb{Z})^\times \times (\mathbb{Z}/\mathbb{Z})^\times \cong (\mathbb{Z}/2^d\mathbb{Z})^\times$ איבר יוצר

קיים שם g^{φ} עבור g^{φ}. אם g כזה או כזה, אז $g+g$ הוא או כזה אז שם עבור g^{φ}.

אבל יש שם $g \in \mathbb{Z}$ עבור g^{φ} כך ש- g או כזה. אבל $\overline{g} \in (\mathbb{Z}/2^d\mathbb{Z})^\times$ והוא

יוצר של $(\mathbb{Z}/2^d\mathbb{Z})^\times$.

* **מה השורה:** אם m אותר (כזה שם עבור φ וכזה שבה) אז $m = m_1 \cdot m_2$

כאשר m_1, m_2 כזרים, $a \in m_1$, $a \in m_2$ (ההוכחה מכ.ת!).

יהי $a \in \mathbb{Z}$. $\gcd(a,m)=1$. אז $a^{\varphi(m)} \equiv 1 \pmod{m}$ כי $\gcd(m_1,m_2)=1$

$\varphi(m_1)$ כזה, $\varphi(m_2)$ כזה. $\varphi(m) = \varphi(m_1)\varphi(m_2)$

$$a^{\frac{\varphi(m)}{2}} = a^{\frac{\varphi(m_1)\varphi(m_2)}{2}} \equiv (a^{\varphi(m_1)})^{\frac{\varphi(m_2)}{2}} \equiv 1 \pmod{m_2}$$

$$a^{\frac{\varphi(m)}{2}} \equiv (a^{\varphi(m_2)})^{\frac{\varphi(m_1)}{2}} \equiv 1 \pmod{m_1}$$

לכן $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$ כי $m = m_1 \cdot m_2$ ← הכפל של a אינו $\frac{\varphi(m)}{2}$ ונקן אין שם! ∎

דוגמא

יש שורש פרימיטיבי עבור: 1, 2, 4, 7, 49, 98, 3, 9, 27, 18, 14

אין שם עבור: 16, 8, 32, 24

שאריות מחלקות n-ית:

הגדרה: אם $w \in \mathbb{Z}$, $n \in \mathbb{N}$, $a \in \mathbb{Z}$ ו- $\gcd(a,w)=1$ אז שאומרים ש- a

שארית מחלקה n-ית אם יש פתרון למשוואה: $a \equiv x^n \pmod{w}$ ⊛

דוגמא: 2 היא שארית מחלקה 2 (ריבועית) מודולו 7 כי $3^2 \equiv 2 \pmod{7}$

(אבל 2 הפך ב- $\mathbb{Z}/7\mathbb{Z}$ הוא מחלקה n-ית) ~~מחלקה~~

תרגול 11 – השארית הריבועית

הקריטריון של אוילר מופלג (אוילר: $n=2$)

משפט: אם m טבעי ו־$\gcd(a,m)=1$ אז a הוא שארית ריבועית מודולו m $\iff$ $a^{\varphi(m)/d}\equiv 1\ (m)$ כאשר $d=\gcd(n,\varphi(m))$.

הוכחה בשיעור הבית!

דוגמא: ① $m=7$, $n=3$. $x^3\equiv a\ (7)$

$\varphi(m)=\varphi(7)=6$. $\gcd(\varphi(m),n)=\gcd(6,3)=3$ $\quad \varphi(n)/d=6/3=2$

לפי המשפט, שקילות $\iff$ $a^2\equiv 1\ (7)$.

נבדוק:

a	1	2	3	4	5	6
a^2	1	4	2	2	4	1

$\Leftarrow$ $a^2\equiv 1\ (7)$: $a=1,6$

x	1	2	3	4	5	6
x^3	1	1	6	1	6	6

$\surd$

⚠ אמנם, שקילות, אבל, p במשקלה זה $3=p$ שקילות

② $m=7$, $n=2$. $x^2\equiv a\ (7)$

לפי המשפט, שקילות $\iff$ $a^3\equiv 1\ (7)$ $\rightarrow$ לפי הדוגמא הקודמת: $a=1,4,2$