תרגול 6

הגדרה: תהי G חבורה, $x\in G$. $\langle x\rangle = \{x^n \mid n\in\mathbb{Z}\} = \{\dots x^{-2}, x^{-1}, x, x^2, \dots\}$

תת החבורה הנוצרת ע"י x.

הגדרה: $x\in G$ נקרא **יוצר** של G אם $G=\langle x\rangle$

הגדרה: $x\in G$ נקרא **מחזורי** (או מסדר סופי) אם יש n כזה.

משפט: תהי G חבורה, $x\in G$ איבר מסדר סופי n אז $|\langle x\rangle| = n$

הוכחה: כותבים $\langle x\rangle = S = \{1, x, \dots x^{n-1}\}$. צ"ל S סופן.

צ"ל כפל סגור, $x^i \cdot x^j = x^k$ כאשר $0\le i,j<n$

$0 < i+j < 2n-2$ ולכן כדי כך $\operatorname{ord}(x)=n$

$x^{i+j} = x^{i+j-n}$

$x^n = x^{kq+r} = x^r$ $\forall n$ $r<n$ $n=kq+r$

ולכן הכלה בין כיוונית, $\langle x\rangle = S_x \Rightarrow n = |\langle x\rangle|$ ∎

לכן אם $x\in G$, G חבורה סופית:

x יוצר $\Leftrightarrow G=\langle x\rangle \Leftrightarrow |\langle x\rangle| = |G| \Leftrightarrow \operatorname{Ord}(x)=|G|$

לכן G חבורה **ציקלית** $\Leftrightarrow \exists x\in G : \operatorname{ord}x = |G|$

דוגמא: $\mathbb{Z}_8^\times = \{\bar1, \bar3, \bar5, \bar7\}$ $\Rightarrow$ אין איבר מסדר 4 וזה חבורה אינה ציקלית!
$\operatorname{ord}:\ 1\ \ 2\ \ 2\ \ 2$

? עבור אילו m $\mathbb{Z}_m^\times$ ציקלית

הגדרה: **שורש פרימיטיבי** modulo m (או מודולו m) הוא מס' $a\in\mathbb{Z}$ כך ש- $\gcd(a,m)=1$ ו- $\bar a \in \mathbb{Z}_m^\times$ הינו יוצר.

דוגמא: 2 שורש פרימיטיבי של 5:

$\bar1 \to \bar2 \to \bar4 \to \bar3 \to \bar1$ $\quad \operatorname{ord}(\bar2)=4$ $\quad |\mathbb{Z}_5^\times| = 4$

הוא קל שורש פרימיטיבי מודולו $\mathbb{Z}_8^\times$ אין כלל!

משפט השאריות הסיני

טענה 1: אם $a_1,..,a_e \in \mathbb{Z}$, $\gcd(a_i,m)=1$ לכל i אז $\gcd(\prod_{i=1}^{e} a_i, m)=1$

הוכחה: אחרת $\gcd(\prod a_i, m) \neq 1$

אז קיים ראשוני p כך ש- $p \mid m$ ו $p \mid \prod a_i$

* את הראשוני מחפשים, הוא מחלק לפחות אחד מהם.

אז $p \mid a_j$ עבור j כלשהו $\Rightarrow$ סתירה!

טענה 2: יהי n $\forall 1 \leq i \leq t,\ a_i \mid n$ ו $\forall i \neq j\ \gcd(a_i,a_j)=1$

אזי $n \mid \tilde{\prod_{i=1}^{t}} a_i$

הוכחה: באינדוקציה על t

$t=1$ טריוויאלי.

צעד - נכון $a_1 \cdot \ldots \cdot a_{t-1} \mid n$ ו $\gcd(a_t, \underbrace{a_i \cdot \ldots \cdot a_{t-1}}_{\text{מכפלה } 1}) = 1$

לפי הנ"א שמתקיים u,s : $s a_t + s(a_i \cdot \ldots \cdot a_{t-1}) = 1$

$$n \cdot s a_t + n s a_i \cdot \ldots \cdot a_{t-1} = n$$

לכן בראשון $a_1 \cdot \ldots \cdot a_t \mid n s a_1 \cdot \ldots \cdot a_{t-1}$ ו $a_t \mid n \cdot s a_t$

כנדרש! ∎

המשך תוס' 6:

משפט השאריות הסיני: יהי $m=m_1\cdots m_t$, $m_i\in\mathbb{Z}$, $m_i>1$

$b_1,b_2,\ldots b_t\in\mathbb{Z}$ אזי $\gcd(m_i,m_j)=1$ עבור $i\neq j$. קיים $x\in\mathbb{Z}$ מהצורה

$x\equiv b_i(m_i)$ לכל $1\le i\le t$, $x\in\mathbb{Z}$

הקיבוץ הזה יחיד מודולו m.

הוכחה: נגדיר $n_i=\prod_{j\neq i}m_j$ ($n_i=m/m_i$).

לפי למה 1 $\gcd(m_i,n_i)=1$. לכן קיימים $r_i,s_i\in\mathbb{Z}$ כך ש- $r_im_i+s_in_i=1$

נגדיר $e_i=s_in_i\in\mathbb{Z}$. אזי $e_i\equiv 1\,(m_i)$ ו $e_i\equiv 0\,(m_j)$ לכל $j\neq i$

$$e_i=s_in_i=s_i\prod_{j\neq i}m_j$$

נגדיר $x_0=\sum_{i=1}^{t}b_ie_i\in\mathbb{Z}$. אזי $x_0\equiv b_ie_i\,(m_i)$ $\forall i$

כי $e_j\equiv 0\,(m_i)$ עבור $i\neq j\Rightarrow x_0\equiv b_i\,(m_i)$ כי $e_i\equiv 1\,(m_i)$

ולכן $x_0\equiv b_1\,(m_1)$

$x_0\equiv b_2\,(m_2)$

$\vdots$

$x_0\equiv b_n\,(m_n)$ כלכלה!

יהי x_1 פתרון אחר. אזי $x_0-x_1\equiv 0\,(m_i)$ $\forall i$:

מנ"א אחרת $m_i\mid x_0-x_1$ לפי למה 2. $m\mid(x_0-x_1)$ ◻

דוגמא: הסינ. סון בן-אוצה: מצא מס' כך שהשאריות מחלוקה ב- 3,5,7 הן 2,3,2 בהתאמה.

פתרון: $m_3=7$, $m_2=5$, $m_1=3$. $m=m_1m_2m_3=3\cdot5\cdot7=105$

$n_1=35$, $n_2=21$, $n_3=15$ ← $r_1m_1+s_1n_1=1$

$r_1\cdot 3+s_1\cdot 35=1$

$s_1\cdot 35\equiv 1\,(3)$ ⇒ $e_1=s_1n_1=2\cdot 35=70$

$s_1\cdot 2\equiv 1\,(3)$

$2\cdot 2\equiv 1\,(3)$

$s_1=2$

בדומה: $s_2\cdot 21\equiv 1\,(5)$ $\quad s_3\cdot 15\equiv 1\,(7)$

$s_2=1$ $\quad s_3=1$

$e_2=s_2\cdot 21=21$ $\quad e_3=1\cdot 15=15$

תשובה: $x=2\cdot 70+3\cdot 21+2\cdot 15=233$

מודולו 105: $x=233\equiv 23\,(105)$

בודקת: $23\equiv 2\,(3)$

$23\equiv 3\,(5)$

$23\equiv 2\,(7)$ ✓

⊛
$$\begin{cases} 6x \equiv 9 \ (15) \\ 4x \equiv 1 \ (7) \end{cases}$$

$6x \equiv 9 \ (15)$
$\gcd(6,15) = 3$
$6x - 15y = 9$
$2x - 5y = 3$
$2x \equiv 3 \ (5)$
$2x \equiv -2 \ (5)$
$x \equiv -1 \ (5)$
$x \equiv 4 \ (5)$

אכן הפתרונות הם: $4, 4+5, 4+10 \ (15)$ ← שלושה!

$x \equiv -1 \ (5)$

~~[illegible]~~

$4x \equiv 1 \ (7)$
$\gcd(4,7) = 1$ יש פתרון
$x \equiv 2 \ (7)$

ומכאן נמשיך באלגוריתם של משפט השאריות הסיני:

$$\begin{cases} x \equiv -1 \ (5) \\ x \equiv 2 \ (7) \end{cases}$$

(שים לב כי עדיין מהפתרונות כי $\gcd(4,6) \neq 1$)

טענה: אם $\gcd(m_1, m_2) = 1$ אז $\varphi(m_1 m_2) = \varphi(m_1) \cdot \varphi(m_2)$

נוכיח יותר מזה: $\mathbb{Z}/m_1m_2\mathbb{Z}^* \cong (\mathbb{Z}/m_1\mathbb{Z})^* \times (\mathbb{Z}/m_2\mathbb{Z})^*$ – משפט השאריות הסיני