יסודות הקריפטוגרפיה תרגול #4

<u>תזכורת</u>:

- בשדה בעל p איברים $\mathbb{Z}_p = \mathbb{Z}\ mod\ p$.
- בשדה בעל p^k איברים: $GF(p^k) = \mathbb{Z}_p[u]\ mod\ f$, כאשר f הוא פולינום מדרגה k מהצורה $a_k u^k + \cdots + a_1 u + a_0$.

משפט:

אם נסתכל על החבורה הכפלית של השדה $GF^*(p^k)$ אז חבורה זו ציקלית. ניסוח שקול: קיים $g \in GF^*(p^k)$ יוצר של החבורה, כלומר $GF^*(p^k) = \left\{g, g^2, \dots, g^{p^k-1} = 1\right\}$.

אולי תמיד u הוא יוצר (שורש פרימיטיבי) של $GF^*(p^k)$? **לא**: ניתן לראות דוגמא בסייג'.

הוכחה:

סימון: $|x|$ יהיה הסדר של x בחבורה $GF^*(p^k)$, כלומר מספר הפעמים המינימלי שיש להעלות את x בחזקה כדי לקבל 1.

נניח בשלילה כי $GF^*(p^k)$ אינה ציקלית וניקח g איבר מסדר מקסימלי $|g| < p^k - 1$. נסתכל על הפולינום $x^{|g|} - 1$. יש זה יש לכל היותר $|g|$ שורשים ב-$GF^*(p^k)$ ולכן יש h עבורו $|h|$ לא מחלק את $|g|$, וזה שקול לכך ש-h אינו שורש של הפולינום. נבחר h כזה מינימלי.

<u>טענה</u>: $|h| = q^l$ עבור q ראשוני כלשהו ו-$l \in \mathbb{N}^*$.

<u>הוכחה</u>: יהיו $|h|$ | q, q' (מחלקים את הסדר של h), q, q' ראשוניים ושונים זה מזה. בה"כ נניח כי q לא מחלק את $|g|$ ולכן $h^{q'}$ איבר מסדר קטן יותר ועדיין $|h^{q'}|$ לא מחלק את $|g|$. נטען כי $q^{l-1}||g|$ (הוכחה דומה). מתקיים: $|g| < |g| \cdot q \underset{=x \cdot q^l}{} = lcm(|g|, q^l) = lcm(|g|, |h|) = m$. נתבונן באיבר $g \cdot h$. מצד אחד $(gh)^m = g^m \cdot h^m = 1 \cdot 1 = 1$ ולכן $|gh||m$. אם $|gh| < m$ אז:

1. מקרה ראשון: $1 = (gh)^{\frac{m}{q}} \overset{=|g|}{=} h^{|g|}$ – סתירה להגדרת h כי h לא אמור להיות שורש הפולינום.
2. מקרה שני: יש ראשוני $q' \neq q$ כך ש-$1 = (gh)^{\frac{m}{q'}} = g^{\frac{m}{q'}} = g^{|g| \cdot \frac{q}{q'}}$, סתירה לכך שהסדר של g הוא $|g|$.

מכאן ש-$|g| < |gh|$, סתירה לבחירת g. □

איך נמצא יוצר:

<u>אבחנה</u>: אם $\gcd(m, p^k - 1) = 1$ ו-g יוצר של $GF^*(p^k)$ אז גם g^m יוצר. לכן יש $\Phi(p^k - 1) < p^k - 1$ (פונקציית אוילר). לכן די לבדוק $\frac{p^k-1}{\log k}$ ביעילות האם איבר נתון הוא יוצר ויהיה לנו אלגוריתם הסתברותי יעיל למצוא איבר יוצר.