

יסודות הקריפטוגרפיה תרגול #4

תזכורת:

- בשדה בעל p איברים $\mathbb{Z}_p = \mathbb{Z} \bmod p$.
- בשדה בעל p^k איברים: $GF(p^k) = \mathbb{Z}_p[u] \bmod f$, כאשר f הוא פולינום מדרגה k מהצורה $a_0 + a_1u + \dots + a_ku^k$.

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 $GF^*(p^k) = \{g, g^2, \dots, g^{p^k-1} = 1\}$.

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

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

הוכחה: יהיו $q, q' | |h|$ (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: $|g| \cdot q > |g| = |g| \cdot q^l$ (כאשר $q^l = x \cdot q^l$). נתבונן באיבר

$g \cdot h$. מצד אחד $1 = 1 \cdot 1 = g^m \cdot h^m = (gh)^m$ ולכן $|gh| |m|$. אם $|gh| < m$ אז:

1. מקרה ראשון: $|gh| = h^{|g|} = (gh)^{\frac{|g|}{q}} = 1$ – סתירה להגדרת h כי h לא אמור להיות שורש הפולינום.

2. מקרה שני: יש ראשוני $q \neq q'$ כך ש- $q^l = g^{|g| \cdot \frac{q}{q'}} = (gh)^{\frac{m}{q}} = 1$, סתירה לכך שהסדר של g הוא $|g|$.

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

איך נמצא יוצר:

אבחנה: אם $\gcd(m, p^k - 1) = 1$ ו- g יוצר של $GF^*(p^k)$ אז גם g^m יוצר. לכן יש $p^k - 1 < \Phi(p^k - 1) = \frac{p^k - 1}{\log k}$ (פונקציה אויילר). לכן די לבדוק

ביעילות האם איבר נתון הוא יוצר ויהיה לנו אלגוריתם הסתברותי יעיל למצוא איבר יוצר.