

**יסודות הקריפטוגרפיה תרגול #3**

המציין של שדה סופי: מספר הפעמים שצריך לחבר 1 לעצמו כדי לקבל 0. המציין הזה תמיד ראשוני לכל שדה סופי.

המציין של  $GF(p^k)$  הוא  $\mathbb{Z}_p$ .  $GF(p) = \mathbb{Z}_p$ , פעולות כפל וחיבור מודולו  $p$ .

$GF(p^k)$ : נסמן את החבורה הכפלית של שדה  $F$  ב- $F^*$ . נסמן  $F = GF(p^k)$ , אז  $F^*$  בעל  $q = p^k - 1$  איברים.

משפט לגרנג'י: לכל  $a \in F^*$  הסדר של  $a$ , נסמנו  $n$  מחלק את  $q$ :  $n|q$ .

נניח ש- $ord_{F^*}(a) = l$ , וגם  $a^l = 1$ . לא יתכן  $l < j$  אז  $l$  לא מינימלי. נסתכל על  $j \bmod l$ :

$$1 = a^j = a^{j \bmod l} \Rightarrow j \bmod l = 0 \Rightarrow l|j$$

**Primitive elements in  $GF^*(p^k)$** 

טענה:  $F^*$  היא חבורה ציקלית, כלומר קיים  $g \in F^*$  כך ש- $F^* = \{g, g^2, \dots, g^{p^k-1}\}$  (הסימון כמו לעיל  $(F^* = GF^*(p^k))$ ). איבר  $g$  זה נקרא איבר

פרימיטיבי של  $F^*$ . טענה זו לא נכונה בשדות אינסופיים כמו  $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ .

**אריתמטיקה של פולינומים:**

יש לא מעט אנלוגיות בין מספרים טבעיים ובין פולינומים:

א. גודל (מס' ביטים בטבעיים, דרגה בפולינומים).

ב. שאריות: נניח  $f(x), g(x)$  ( $\deg(f) \geq \deg(g)$ ) שני פולינומים מעל שדה. קיימים שני פולינומים  $h(x), r(x)$  יחידים כך ש-  $f(x) = h(x) \cdot g(x) + r(x)$

ו- $\deg(r) < \deg(g)$ . במספרים:  $F = H \cdot G + R$  (עבור מספרים).

ג. GCD: מוגדר על פולינומים ועל מספרים.

ד. ראשוניות: מספר ראשוני לעומת פולינום אי פריק. מהצד השני: פירוק לגורמים.

נניח כי  $f(x)$  פולינום אי פריק מדרגה  $k$  מעל  $GF(p^k)$ . שדה זה ניתן לייצוג ע"י פולינומים מדרגה  $k-1$  (או פחות) מעל  $GF(p)$  (יש  $p^k$  כאלה  $k$  - מקדמים ו- $p$  אפשרויות לכל מקדם).

אם  $f$  פולינום מדרגה  $k$  ו- $g, h$  פולינומים מדרגה  $k-1$ , להכפלתם:  $g \cdot h \bmod f$  - מתקבל פולינום מדרגה  $k-1$  (חישוב שארית לפולינום מדרגה

$$2k - 2 \text{ ביחס לפולינום מדרגה } k \text{ יתן } k - 1 = 2k - 2 - (k - 1).$$