תרגיל מספר 12 מבנים אלגבריים

1.

(א) הוכיחו כי $f(x)=x^2+x+4\in\mathbb{Z}_{11}[x]$ ראשוני ולכן $\mathbb{F}=\mathbb{Z}_{11}[x]/\left\langle x^2+x+4\right\rangle$ שדה.

(ב) מצאו $[3x+2]^{-1}$ ב $\mathbb{F}$ הנ"ל.

2. יהי $\mathbb{F}=\mathbb{F}_{2^n}$ שדה סופי הוא מקיים כי $1+1=0$. הוכיחו כי כל איבר בו הוא ריבוע כלומר $\forall x\in\mathbb{F}\exists y\in\mathbb{F}:\ x=y^2$.
הדרכה: נגדיר העתקה : $\phi:\mathbb{F}\to\mathbb{F}$ ע"י $\phi(x)=x^2$ הראו שהעתקה זו היא חח"ע והסיקו כי ϕ על ולכן הטענה מתקיימת.

3. יהא $\mathbb{F}=\mathbb{F}_{p^n}$ שדה עם p^n איברים. הוכיחו כי

$$x^{p^n-1}-1=\prod_{\alpha\in\mathbb{F}^\times}(x-\alpha)$$

כאשר השיוון הוא שיוון פולינומים ו $\mathbb{F}^\times=\mathbb{F}\setminus\{0\}$.
הסיקו את משפט וילסון: יהא p מספר ראשוני אי זוגי אזי

$$(p-1)!\equiv -1\mod p$$