

תרגיל בית סמינר בתורת המספרים 1

31 באוקטובר 2018

שאלה 1

בצעו חלוקה עם שארית, כלומר כתבו

$$f = qg + r$$

כאשר

$$\deg(r) < \deg(g)$$

במקרים הבאים:

- | | | | |
|----|--------------------|-----------------------|-----------------|
| 1. | $F = \mathbb{Z}_5$ | $f(x) = x^2 + 2x - 1$ | $g(x) = x + 3$ |
| 2. | $F = \mathbb{Z}_3$ | $f(x) = x^3 + 2x + 1$ | $g(x) = 2x + 1$ |

שאלה 2

מצאו את $\gcd(f, g)$ במקרים הבאים:

- | | | | |
|----|--------------------|----------------------|-------------------|
| 1. | $F = \mathbb{Z}_3$ | $f(x) = x^3 + x + 1$ | $g(x) = x + 2$ |
| 2. | $F = \mathbb{Z}_5$ | $f(x) = x^2 - x + 3$ | $g(x) = x^2 + 3x$ |

שאלה 3

פרקו את הפולינומים הבאים למכפלת אי פריקים:

- | | | |
|----|--------------------|-------------------------|
| 1. | $F = \mathbb{Z}_5$ | $f(x) = x^2 + 2x + 1$ |
| 2. | $F = \mathbb{Z}_3$ | $f(x) = x^3 + x^2 + 2x$ |

שאלה 4

מעל השדה

$$F = \mathbb{Z}_3$$

מצא פולינום כבמשפט השאריות הסיני $f(x)$ כך שעבור

$$m_1 = x^2 + 1$$

$$m_2 = x + 1$$

מתקיים

1. $f(x) \equiv x + 1 \pmod{(m_1)}$
2. $f(x) \equiv 2 \pmod{(m_2)}$

שאלה 5

מעל השדה

$$F = \mathbb{Z}_3$$

מצאו הופכי ל- $x + 2$ מודולו $x^2 + x$, כלומר $a(x)$ כך ש-

$$a(x)(x + 2) \equiv 1 \pmod{(x^2 + x)}$$