3. ŽIEDAI IR IDEALAI

UŽDAVINIAI.

1.1. Raskite visus žiedų homomorfizmus $f: Z_n \to Z_m$.

1.2. Raskite visus pirminius ir visus maksimalius žiedo $Z_m = Z/mZ$ idealus.

2. Raskite visus 3-iojo laipsnio neredukuojamus polinomus virš kūno $GF(13)$.

3.1. Parašykite daugybos lentelę žiede $R = GF(p)[x]/(m(x))$, kai $m(x)$ yra redukuojamas s-ojo laipsnio polinomas virš kūno $GF(p)$.

3.2. Raskite visus žiedo R idealus.

3.3. Raskite visus žiedo R vieneto daliklius.

PARAMETRAI.

1.1. 1 grupei : $n = 3^{a_1} \cdot 5^{b_1} \cdot 7^{c_1}, m = 5^{a_2} \cdot 7^{b_2} \cdot 11^{c_2}$,

2 grupei : $m = 3^{a_1} \cdot 5^{b_1} \cdot 7^{c_1}, n = 5^{a_2} \cdot 7^{b_2} \cdot 11^{c_2}$,

3 grupei : $n = 2^{a_1} \cdot 3^{b_1} \cdot 13^{c_1}, m = 2^{a_2} \cdot 5^{b_2} \cdot 13^{c_2}$,

$a_i, b_i, c_i \geq 1; i = 1, 2.$

1.2. m iš 1.1.

2. 3-iojo laipsnio polinomų virš kūno $GF(13)$ yra 13^3. Jų struktūra yra

$f(x) = x^3 + ax^2 + bx + c;\ 0 \leq a, b, c \leq 12.$

Tegu $n = a \cdot 13^2 + b \cdot 13 + c$, tada polinomų $f(x)$ koeficientus a, b, c parinkite taip, kad

3 grupei : $0 \leq n \leq 732$,

2 grupei : $733 \leq n \leq 1464$,

1 grupei : $1465 \leq n \leq 2197$.

3.1. 1 grupei $p = 5, s \geq 5$,

2 grupei : $p = 7, s \geq 5$,

3 grupei : $p = 11, s \geq 5$.

PATARIMAI.

1.1. Žiedų homomorfizmas $f: Z_n \to Z_m$ turi tenkinti dvi sąlygas :

1) adityvi elemento $e = f(\overline{1})$ eilė turi būti $d =$BDD(m, n) daliklis . Todėl elementas e turi būti pogrupyje $\frac{m}{d}Z = \left\{0, \frac{m}{d} \cdot 1, ..., \frac{m}{d} \cdot (d-1)\right\}$.

2) elementas e turi būti idempotentas žiede Z_m : $e^2 = e$.

1.2, 3.2. 1) Pasinaudoti teorema:

Tegu R/I yra žiedo R faktoržiedis idealo I atžvilgiu. Tada egzistuoja bijektyvi funkcija tarp žiedo R/I idealų ir žiedo R idealų, kurių poaibiu yra idealas I .

2) Neužmirškite, kad žiedai Z ir $GF(p)[x]$ yra pagrindinių idealų sritys.