5. BAIGTINIAI KŪNAI IR NEREDUKUOJAMI POLINOMAI.

UŽDAVINIAI.

1. Raskite antrojo laipsnio neredukuojamus polinomus $x^2 + a_1 x + a_0 \in GF(p)[x]$ ir jų eiles. Kurie iš šių polinomų yra primityvieji? Kodėl?

2. Pasirinkite primityvųjį neredukuojamą polinomą $f(x)$ iš 1. Parašykite indeksų lentelę kūno $GF(p^2) = GF(p)(a)$, čia a - polinomo $f(x)$ šaknis, elementams.

3. Faktorizuokite du polinomus iš 1. kūne $GF(p^2) = GF(p)(a)$.

4. Su kuriais $b \in GF(p^2) = GF(p)(a)$ lygtis $x^2 - b = 0$ yra išsprendžiama.

5. Ar iš gautų 4. elementų galima ištraukti 3-ojo laipsnio šaknį. Kodėl?

PARAMETRAI.

1 grupei $p = 17$:

$a_0 = 3, 5, 6, 7, 10, 11, 12, 14.$

$a_1 \in [1, 8], [9, 16].$

$p = 29$:

$a_0 = 18, 21, 26.$

$a_1 \in [1, 9], [10, 16], [17, 22], [22, 28].$

2 grupei $p = 19$:

$a_0 = 2, 3, 10, 13, 14, 15.$

$a_1 \in [1, 6], [7, 12], [12, 18].$

$p = 29$:

$a_0 = 11, 14, 15.$

$a_1 \in [1, 9], [10, 16], [17, 22], [22, 28].$

3 grupei $p = 23$:

$a_0 = 5, 7, 10, 11, 14.$

$a_1 \in [1, 5], [6, 10], [11, 15], [16, 22].$

$p = 29$:

$a_0 = 8, 10.$

$a_1 \in [1, 9], [10, 16], [17, 22], [22, 28].$

4 grupei $p = 23$:

$a_0 = 15, 17, 19, 20, 21.$

$a_1 \in [1, 5], [6, 10], [11, 15], [16, 22].$

$p = 29$:

$a_0 = 2, 3.$

$a_1 \in [1, 9], [10, 16], [17, 22], [22, 28].$