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 neprimityvųjį neredukuojamą polinomą iš 1. ir primityvųjį polinomą iš 1. Parašykite indeksų lentelę kūno $GF(p^2)$ elementams.

PARAMETRAI.

1 grupei $p = 29$.

$a_0 = 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.$

$a_1 \in [1, 10], [11, 19], [20, 28]$.

2 grupei $p = 31$.

$a_0 = 3, 11, 12, 13.$

$a_1 \in [1, 5], [6, 8], [9, 12], [13, 16], [17, 21], [22, 25], [23, 30]$.

3 grupei $p = 31$.

$a_0 = 17, 21, 22, 24.$

$a_1 \in [1, 5], [6, 8], [9, 12], [13, 16], [17, 21], [22, 25], [23, 30]$.