

## 6. VIENETO ŠAKNYS IR CIKLOTOMINIAI POLINOMAI

### UŽDAVINIAI.

1. Polinomo  $x^n - 1$  faktorizacija virš kūno  $GF(q)$  .

1.1. Sudarykite ciklotomines aibes moduliu  $n$  .

1.2. Kiek neredukuojamų polinomų yra polinomo  $x^n - 1$  kanoniniame skaidinyje ir kokie šių polinomų laipsniai .

1.3. Faktorizuokite polinomą  $x^n - 1$  virš kūno  $GF(q)$  .

2. Ciklotominiai polinomial.

2.1. Užrašykite polinomą  $x^n - 1$  ciklotominių polinomų sandauga.

2.2. Raskite ciklotominius polinomus iš 2.1.

2.3. Ciklotominiams polinomams iš 2.2 patikrinkite lygybes:

(i)  $Q_{np}(x) = Q_n(x^p)/Q_n(x)$ , kai  $p$  nėra  $n$  daliklis;

(ii)  $Q_{np}(x) = Q_n(x^p)$ , kai  $p$  yra  $n$  daliklis;

(iii)  $Q_{np^k}(x) = Q_{np}(x^{p^{k-1}})$ ;

(iv)  $Q_n(x^{-1})x^{\varphi(n)} = Q_n(x)$ ,  $n \geq 2$ , čia  $\varphi(n)$  - Oilerio funkcija.

2.4. Apskaičiuokite ciklotominių polinomų iš 2.1 reikšmes:  $Q_n(0)$ ,  $Q_n(1)$ ,  $Q_n(-1)$ .

3.1. Pateikite ne mažiau kaip penkis kūno  $GF(q)$  plėtinius virš kurių neredukuojami polinomial iš 1.3 liks neredukuojamais polinomial .

3.2. Pateikite ne mažiau kaip penkis kūno  $GF(q)$  plėtinius virš kurių neredukuojami polinomial iš 1.3 taps redukuojamais polinomial .

3.3. Virš kurio nors iš kūnų iš 2.4 faktorizuokite redukuojamais tapusius polinomus iš 1.3.

### PARAMETRAI.

Visoms grupėms :  $DBD(n, q) = 1$  .

1 grupei  $q = 4$  ,  $n \geq 25$  .

2 grupei  $q = 2$  ,  $n \geq 25$ .

3 grupei  $q = 3$  ,  $n \geq 20$ .

4 grupei  $q = 9$  ,  $n \geq 15$ .