Tópicos Avançados em Ciência da Computação I:
Introdução à Teoria de Códigos para Criptografia Pós-Quântica
Prof. Daniel Panario

Lista de Exercícios II
Entrega: Sexta Feira 31 de janeiro de 2020
Valor no curso: 20%

1. (10 pontos) Determine o menor inteiro q, potência de um primo, e inteiro positivo n, para os quais I_n/q^n satisfaz

$$\frac{1}{2n} \leq \frac{I_n}{q^n} \leq \frac{1}{n} \quad .$$

Dê uma tabela com valores de (q, n) para vários valores de q.

2. (15 Marks) É sabido que, para cada corpo finito $\mathbb{F}_q$ e cada $n \in \mathbf{N}$, o produto de todos os polinômios irredutíveis mônicos sobre $\mathbb{F}_q$ com grau dividindo n é igual a $x^{q^n} - x$. Usando esse resultado, encontre a fatoração completa dos seguintes polinômios:

$$(a)\ x^{16} - x \text{ sobre } \mathbb{F}_2; \qquad (b)\ x^{32} - x \text{ sobre } \mathbb{F}_2; \qquad (c)\ x^9 - x \text{ sobre } \mathbb{F}_3.$$

3. (10 pontos) Use o material sobre testes de irredutibilidade, dado em aula, para determinar se o polinômio $x^8 + x^6 + x^3 + x + 1$ é irredutível sobre $\mathbb{F}_2$.

4. (15 pontos) Prove que

$$\text{mdc}\left(x^{q^i} - x, f\right) = \text{mdc}\left(\left(x^{q^i} - x\right) \bmod f, f\right).$$

5. (15 pontos) Seja $g(x) = x^3 + x + 1$ o polinômio gerador de um código binário linear cíclico de comprimento 7.

(a) **(3 pontos)** Codifique as seguintes mensagens (polinômios): $x^3 + 1$, x, $x^3 + x^2 + x$.

(b) **(12 pontos)** Encontre o polinômio (mensagem) correspondente às palavras código: $x^5 + x^2 + x + 1$, $x^4 + x^3 + x^2 + 1$, $x^6 + x^5 + x^3 + 1$.

6. (20 pontos)

(a) **(8 pontos)** Encontre as classes laterais ciclotômicas para $p = 2$ e $m = 5$ (assim $n = 31$), e para $p = 3$ e $m = 3$ (assim $n = 26$).

(b) **(12 pontos)** Encontre o polinômio minimal de dois elementos de $\mathbb{F}_{2^5}$ em classes laterais ciclotômicas diferentes no corpo $\mathbb{F}_{2^5}$, construído usando $x^5 + x^2 + 1$. (Os elementos devem pertencer a $\mathbb{F}_{2^5}$ mas nao podem estar em $\mathbb{F}_2$.)

7. (15 Pontos) Neste exercício vamos rever o exemplo de LFSR da aula.
Seja a sequência $\{s_k\}$ em $\mathbb{F}_2$ definida por

$$s_{k+4} = s_{k+3} + s_k, \quad k \geq 0, \quad s_0 = s_1 = s_2 = 0,\ s_3 = 1.$$

(a) **(3 Pontos)** Dê a figura do LFSR nesse caso.

(b) **(6 Pontos)** Dê o polinômio característico f e a matriz companheira A.

(c) **(6 Pontos)** Dê a sequência obtida usando a semente 1000. Qual é a sequência obtida usando quaisquer sementes não nulas (ou seja, sementes diferentes de 0000)?