JOSÉ ARMANDO OLIVEIRA MENDES

A fatoração de $x^n - 1$ em binômios e trinômios irredutíveis sobre os corpos com 2 e 4 elementos

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
2025

JOSÉ ARMANDO OLIVEIRA MENDES

A fatoração de $x^n - 1$ em binômios e trinômios irredutíveis sobre os corpos com 2 e 4 elementos

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica.

Orientador: Prof. Dr. Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2025

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

M538 Mendes, José Armando Oliveira, 2000-
2026 A fatoração de xn-1 em binômios e trinômios irredutíveis sobre os corpos com 2 e 4 elementos [recurso eletrônico] / José Armando Oliveira Mendes. - 2026.

Orientador: Victor Gonzalo Lopez Neumann.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
DOI http://doi.org/10.14393/ufu.di.2026.219
Inclui bibliografia.

1. Matemática. I. Neumann, Victor Gonzalo Lopez,1974-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 158 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.ppmat.ime.ufu.br - pgmat@ime.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 127, PPGMAT				
Data:	19/02/2026	Hora de início:	10:00	Hora de encerramento:	12:00
Matrícula do Discente:	12412MAT004				
Nome do Discente:	José Armando Oliveira Mendes				
Título do Trabalho:	A fatoração de x^n-1 em binômios e trinômios irredutíveis sobre os corpos com 2 e 4 elementos				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Propriedades de elementos especiais em corpos finitos				

Reuniu-se por videoconferência, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Abílio Lemos Cardoso Júnior - Universidade Federal de Viçosa / UFV, Cícero Fernandes de Carvalho - Universidade Federal de Uberlândia / UFU e Victor Gonzalo Lopez Neumann - Instituto de Matemática e Estatística - IME/UFU orientador do candidato.

Iniciando os trabalhos o presidente da mesa, Dr. Victor Gonzalo Lopez Neumann apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao discente a palavra para a exposição do seu trabalho.

A duração da apresentação do discente e o tempo de arguição e resposta foram conforme as normas do Programa. A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o candidato:

Aprovado.

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação

interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 19/02/2026, às 21:46, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Cícero Fernandes de Carvalho**, **Professor(a) do Magistério Superior**, em 20/02/2026, às 17:53, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Abílio Lemos Cardoso Júnior**, **Usuário Externo**, em 25/02/2026, às 14:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7044909** e o código CRC **404FB536**.

Referência: Processo nº 23117.006758/2026-97 SEI nº 7044909

Agradecimentos

Agradeço primeiramente a Deus pela vida com saúde e pelas oportunidades a mim concedidas.

Agradeço a toda minha família, em especial à minha mãe, Rosimeire; às minhas tias: "Lena" (*in memoriam*), "Tê" (*in memoriam*), "Lú" e "Pá"; ao tio "Dé"; e à minha prima Marília. Vocês são a minha base, me apoiam e incentivam incondicionalmente, atitudes essenciais para que a jornada do mestrado tenha sido tranquila, sem pressões ou julgamentos, apenas energias positivas vinham de vocês. A vida, no geral, é muito mais leve assim.

Agradeço aos meus amigos: Ana, Danilo e Yara. Vocês também são peças importantes para tudo isso, não necessariamente para a trajetória do mestrado, mas para a minha vida como um todo.

Agradeço aos meus professores da licenciatura no IFGoiano, em especial aos professores Davidson e Dassael. Além de sempre acreditarem na minha capacidade e me motivarem, foram fundamentais para que eu aprendesse a estudar matemática, e também me proporcionaram uma formação inicial sólida, o que me possibilitou enfrentar as disciplinas do mestrado sem grandes dificuldades.

Agradeço aos professores do PPGMAT-UFU, por todos os ensinamentos e contribuições para a minha formação. Em especial, ao meu orientador, Prof. Dr. Victor Gonzalo, pela orientação (sempre com bom humor), paciência e por todos os ensinamentos durante este período de mestrado. Aproveito para estender os agradecimentos à minha banca examinadora, composta pelos professores Dr. Cícero Carvalho e Dr. Abílio Lemos, por todas as contribuições oferecidas para a melhoria do meu trabalho.

Agradeço aos colegas de mestrado, por todos os momentos de estudo e descontração. Em especial, à minha amiga Yara, fiel colega de estudos desde a licenciatura.

Agradeço também à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pelo auxílio financeiro, que tornou possível a realização do mestrado.

MENDES, J. A. O. *A fatoração de $x^n - 1$ em binômios e trinômios irredutíveis sobre os corpos com 2 e 4 elementos.* 2025. (48 pág) Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Sejam q uma potência de um primo e $\mathbb{F}_q$ o corpo finito com q elementos. A fatoração de polinômios sobre corpos finitos desempenha papel fundamental em diversas áreas, como a teoria dos códigos corretores de erros e a criptografia. Um polinômio particularmente importante é $x^n - 1$, pois, por exemplo, cada um de seus fatores irredutíveis representa um código cíclico. Sob certas condições, o polinômio $x^n - 1$ se fatora exclusivamente em binômios e trinômios irredutíveis sobre $\mathbb{F}_q$. Nesse caso, dizemos que o par (n, q) é 3-sparse. O objetivo deste trabalho é classificar completamente os pares $(n, 2)$ e $(n, 4)$ que são 3-sparse.

Palavras-chave: Fatoração, Corpos Finitos, Números p-ádicos, Polinômios Ciclotômicos, Corpos Binários.

MENDES, J. A. O. *A fatoração de $x^n - 1$ em binômios e trinômios irredutíveis sobre os corpos com 2 e 4 elementos.* 2025. (48 pág) Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Abstract

Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. The factorization of polynomials over finite fields plays a fundamental role in several areas, such as error-correcting coding theory and cryptography. A particularly important polynomial is $x^n - 1$, since, for example, each of its irreducible factors corresponds to a cyclic code. Under certain conditions, the polynomial $x^n - 1$ factors exclusively into irreducible binomials and trinomials over $\mathbb{F}_q$. In this case, we say that the pair (n, q) is 3-sparse. The aim of this work is to give a complete classification of the pairs $(n, 2)$ and $(n, 4)$ that are 3-sparse.

Keywords: Factorization, Finite Fields, p-adic Numbers, Cyclotomic Polynomials, Binary Fields.

Lista de Símbolos

$\mathbb{Z}_p$	anel dos inteiros p-ádicos
$\mathbb{F}_q$	corpo finito com q elementos
$\mathbb{Q}_p$	corpo dos números p-ádicos
φ	função de Euler
$[K : F]$	grau de K sobre F
$\partial(f(x))$	grau do polinômio $f(x)$
$\langle a \rangle$	grupo cíclico gerado por a
$\Phi_n(x)$	n-ésimo polinômio ciclotômico
$\mathrm{ord}_b(a)$	ordem de a módulo b
$\lvert a \rvert$	ordem do elemento a
$\lvert G \rvert$	ordem do grupo G
$\mathrm{rad}(n)$	produto dos primos distintos que dividem n

Sumário

Introdução

Sejam q uma potência do primo e $\mathbb{F}_q$ o corpo finito com q elementos. O estudo da fatoração de polinômios sobre $\mathbb{F}_q$ é um problema clássico na teoria dos corpos finitos, com aplicações em diferentes áreas da matemática e da computação, como a teoria dos códigos corretores de erros e a criptografia. Se n é um inteiro positivo, um polinômio particularmente importante para se estudar a fatoração é $x^n - 1$, pois, por exemplo, cada fator irredutível de $x^n - 1$ representa um código cíclico sobre $\mathbb{F}_q$, veja [14].

A fatoração desse polinômio está intimamente relacionada com a fatoração do d-ésimo polinômio ciclotômico $\Phi_d(x)$, já que $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Nas últimas décadas, muitos autores se dedicaram a estudar as fatorações desses polinômios, como podemos observar em [1, 2, 16].

Em [1], por exemplo, observamos que, sob certas condições, o polinômio $x^n - 1$ se fatora exclusivamente em binômios e trinômios irredutíveis sobre $\mathbb{F}_q$. Nesse caso, diremos que o par ordenado (n, q) é 3-sparse. Nesta dissertação, estudaremos o artigo [10] e apresentaremos uma classificação completa dos pares $(n, 2)$ e $(n, 4)$ que são 3-sparse. Para isso estudaremos, primeiro, o artigo [13], para provar um resultado sobre a paridade do número de fatores irredutíveis do polinômio $x^n + x^k + 1$ sobre $\mathbb{F}_2$, que será essencial na classificação desses pares.

Os dois primeiros capítulos deste trabalho são dedicados a apresentar os resultados fundamentais sobre corpos finitos e números p-ádicos que serão essenciais para o desenvolvimento desta dissertação. Para o primeiro tópico, utilizaremos o livro [8] como principal referência, e para o segundo, [5, 6]. No Capítulo 3, investigamos a paridade do número de fatores irredutíveis de trinômios da forma $x^n + x^k + 1$ sobre $\mathbb{F}_2$, utilizando o artigo [13] como referência. Com isso em mãos, no Capítulo 4 caracterizamos os valores de n para os quais o polinômio $x^n - 1$ se fatora exclusivamente em binômios e trinômios sobre $\mathbb{F}_2$ e $\mathbb{F}_4$, adotando o artigo [10] como referência. Além disso, também apresentaremos a fatoração de algumas famílias de polinômios ciclotômicos sobre $\mathbb{F}_2$ e $\mathbb{F}_4$.

É importante salientar que, enquanto esta dissertação estava sendo escrita, Kaimin Cheng classificou totalmente os pares (n, q) que são 3-sparse, para qualquer q, e publicou no arXiv, veja [3, 4].

José Armando Oliveira Mendes

Uberlândia-MG, 19 de Fevereiro de 2025.

Capítulo 1

Corpos Finitos

Este capítulo reúne os resultados fundamentais sobre corpos finitos necessários para o desenvolvimento deste trabalho. Além das propriedades básicas sobre os corpos finitos, apresentaremos também resultados sobre polinômios e, em particular, os polinômios ciclotômicos. Esses polinômios recebem atenção especial pois são extremamente importantes para os resultados principais apresentados no Capítulo 4.

1.1 Corpos Finitos

Definição 1.1. *Um conjunto F é um corpo se ele é um anel comutativo com unidade no qual todo elemento não nulo possui um inverso multiplicativo.*

Definição 1.2. *Sejam F um corpo e n um inteiro positivo tal que $na = 0$, para todo $a \in F$. O menor inteiro positivo n com essa propriedade é chamado de característica de F. Além disso, dizemos que F tem característica n. Se não existe um inteiro positivo n com essa propriedade, dizemos que F tem característica* 0.

Teorema 1.3. *Todo corpo finito tem característica p, em que p é um número primo.*

Demonstração. Veja [8, Corollary 1.45]. □

Teorema 1.4. *Em todo corpo de característica prima p vale a seguinte igualdade:*

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n},$$

para todo inteiro positivo n.

Demonstração. Veja [8, Corollary 1.46]. □

Definição 1.5. *Um conjunto K é subcorpo de um corpo F se $K \subset F$ e K é um corpo com as operações definidas em F. Também dizemos que F é uma extensão de K.*

Definição 1.6. *Um corpo que não tem subcorpos próprios é chamado de corpo primo.*

Exemplo 1.7. *Para todo primo p, o corpo $\mathbb{Z}/p\mathbb{Z}$ é primo. Denotamos esse corpo por $\mathbb{F}_p$.*

Lema 1.8. *Seja F um corpo finito contendo um subcorpo K com q elementos. Então F tem q^m elementos, em que $m = [F : K]$.*

Demonstração. Veja [8, Lemma 2.1]. □

Teorema 1.9 (Existência e Unicidade)**.** *Para todo primo p e todo inteiro positivo n, existe um corpo finito com p^n elementos. Todo corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. Veja [8, Theorem 2.5]. □

Denotaremos o corpo finito com $q = p^n$ elementos por $\mathbb{F}_q$, em que p é a característica desse corpo.

Exemplo 1.10. *O corpo finito $\mathbb{F}_4$ pode ser construído como extensão quadrática de $\mathbb{F}_2$. De fato, consideramos o seguinte polinômio irredutível sobre $\mathbb{F}_2$: $f(x) = x^2 + x + 1$. Seja α uma raiz de $f(x)$, então*

$$\alpha^2 + \alpha + 1 = 0 \implies \alpha^2 = \alpha + 1. \tag{1.1}$$

Assim, $\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha^2\}$. Além disso, sempre que escrevermos $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, fica implícito que α satisfaz a Equação (1.1). Note também que $\mathbb{F}_2$ é o subcorpo primo de $\mathbb{F}_4$.

Teorema 1.11 (Critério de Subcorpo)**.** *Todo subcorpo de $\mathbb{F}_q$ tem ordem p^m, em que m é um inteiro positivo divisor de n. Reciprocamente, se m é um inteiro positivo divisor de n, então existe exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Demonstração. Veja [8, Theorem 2.6]. □

Para o próximo resultado precisaremos de alguns lemas. Nesta dissertação, o símbolo $\sum_{d|n}$ denota a soma sobre todos os divisores positivos d de n.

Lema 1.12. *Para qualquer inteiro positivo n, a função φ de Euler tem a seguinte propriedade:*

$$\sum_{d|n} \varphi(d) = n.$$

Demonstração. Veja [11, Teorema 4.5]. □

Lema 1.13. *Sejam G um grupo e $a \in G$. Valem as seguintes propriedades:*

(i) Se $\langle a \rangle$ é um grupo cíclico de ordem m, então o elemento a^k gera um subgrupo de ordem $m/\operatorname{mdc}(k, m)$.

(ii) O grupo cíclico $\langle a \rangle$ de ordem m possui exatamente $\varphi(m)$ geradores.

Demonstração. Veja [8, Theorem 1.15]. □

Provaremos agora uma das propriedades mais importantes de um corpo finito: o grupo multiplicativo dos elementos não nulos de um corpo finito é cíclico. Faremos isso utilizando o próximo teorema, que é mais geral.

Teorema 1.14. *Seja G um subgrupo finito do grupo multiplicativo dos elementos não nulos de um corpo finito F. Então G é cíclico.*

Demonstração. Sejam $n = |G|$, d um divisor de n e suponhamos que exista $g \in G$ um elemento de ordem d. Posto $H = \langle g \rangle$, temos $|H| = |g| = d$. Pelo item (ii) do lema anterior, H possui $\varphi(d)$ geradores, que são elementos de ordem d.

Seja m_d o número de elementos em G com ordem d. Como todos os elementos de H são raízes de $x^d - 1$ e esse polinômio tem, no máximo, d raízes, concluímos que H contém todas as suas raízes. Ou seja, H contém todos os elementos de G que possuem ordem d. Em H, os elementos de ordem d são precisamente os seus geradores, ou seja, $m_d = \varphi(d)$. Se não existisse nenhum elemento em G com ordem d, teríamos $m_d = 0$. Em geral, $m_d \leq \varphi(d)$.

Definimos $M_d = \{a \in G; |a| = d\}$ o conjunto dos elementos de ordem d. Assim, se d' é um divisor de n diferente de d, então $M_d \cap M_{d'} = \emptyset$. Daí, $G = \cup_{d|n} M_d$ (união disjunta). Logo,

$$n = |G| = \sum_{d|n} |M_d| = \sum_{d|n} m_d \leq \sum_{d|n} \varphi(d) = n.$$

Com isso, $\sum_{d|n} m_d = \sum_{d|n} \varphi(d)$ e, consequentemente, $m_d = \varphi(d)$. Em particular, $m_n = \varphi(n)$, ou seja, G tem $\varphi(n)$ elementos de ordem n. Se g é um desses elementos, segue que $\langle g \rangle = G$, já que $|G| = n$. Isso conclui a demonstração. □

Como consequência imediata desse teorema, vale o seguinte resultado.

Corolário 1.15. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ dos elementos não nulos de $\mathbb{F}_q$ é cíclico.*

Proposição 1.16. *Seja $a \in \mathbb{F}_q$ um elemento de ordem m sobre $\mathbb{F}_q$, isto é, m é o menor inteiro positivo, tal que $a^m = 1$ em $\mathbb{F}_q$. Para todo inteiro positivo k, o elemento a^k tem ordem $\dfrac{m}{\mathrm{mdc}(k,m)}$ sobre $\mathbb{F}_q^*$.*

Demonstração. É apenas outra forma de escrever o item (i) do Lema 1.13. □

Vamos denotar a ordem de a sobre $\mathbb{F}_q^*$ simplesmente por $\mathrm{ord}(a)$.

Definição 1.17. *Um elemento $\alpha \in \mathbb{F}_q$ é chamado de primitivo se ele gera o grupo multiplicativo $\mathbb{F}_q^*$.*

Exemplo 1.18. *No corpo $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, temos $\alpha^2 = \alpha + 1$ e $\alpha^3 = 1$. Donde α tem ordem 3 e, portanto, é um elemento primitivo de $\mathbb{F}_4$.*

1.2 Raízes da Unidade e Polinômios Ciclotômicos

Definição 1.19. *Seja n um inteiro positivo. O corpo de decomposição de x^n-1 sobre um corpo K é chamado de n-ésimo corpo ciclotômico e denotado por $K^{(n)}$. As raízes de x^n-1 em $K^{(n)}$ são chamadas de n-ésimas raízes da unidade sobre K e o conjunto com essas raízes é denotado por $E^{(n)}$.*

A estrutura de $E^{(n)}$ é determinada pela relação entre n e a característica de K, como mostrado no próximo teorema. Utilizaremos p para a característica de K e permitimos $p=0$ também.

Teorema 1.20. *Seja n um inteiro positivo e K um corpo de característica p. Então:*

(i) Se p não divide n, então $E^{(n)}$ é um grupo cíclico de ordem n com respeito a multiplicação em $K^{(n)}$.

(ii) Se p divide n, podemos escrever $n=p^rm$, em que r e m são inteiros positivos e p não divide m. Então $K^{(n)}=K^{(m)}$, $E^{(n)}=E^{(m)}$ e as raízes de x^n-1 em $K^{(n)}$ são os m elementos de $E^{(m)}$, cada um com multiplicidade p^r.

Demonstração. Veja [8, Theorem 2.42]. □

Definição 1.21. *Seja K um corpo de característica p e n um inteiro positivo não divisível por p. Então o gerador do grupo cíclico $E^{(n)}$ é chamado de n-ésima raiz primitiva da unidade sobre K.*

Pelo item (ii) do Lema 1.13, podemos concluir que existem exatamente $\varphi(n)$ n-ésimas raízes primitivas da unidade distintas sobre K. Se ω é uma delas, então todas elas são dadas por ω^s, em que $1\leq s\leq n$ e $\mathrm{mdc}(s,n)=1$. O polinômio cujas raízes são as n-ésimas raízes primitivas da unidade sobre K é de grande interesse e definido a seguir.

Definição 1.22. *Seja K um corpo de característica p, n um inteiro positivo não divisível por p e ω uma n-ésima raiz primitiva da unidade sobre K. Então o polinômio*

$$\Phi_n(x)=\prod_{\substack{s=1\\ \mathrm{mdc}(s,n)=1}}^{n}(x-\omega^s)$$

é chamado de n-ésimo polinômio ciclotômico sobre K.

O polinômio $\Phi_n(x)$ independe da escolha de ω. Além disso, esse polinômio tem grau $\varphi(n)$ e seus coeficientes pertencem à $K^{(n)}$. Nesta dissertação o símbolo $\prod_{d|n}$ denota o produto sobre todos os divisores positivos d de n.

Teorema 1.23. *Seja K um corpo de característica p e n um inteiro positivo não divisível por p. Então*

(i) $x^n-1=\prod_{d|n}\Phi_d(x)$;

(ii) os coeficientes de $\Phi_n(x)$ pertencem ao subcorpo primo de K.

Demonstração. Veja [8, Theorem 2.45]. □

Definição 1.24. *Sejam a, b inteiros positivos, tais que* $\mathrm{mdc}(a,b) = 1$. *Definimos a ordem de a módulo b, e denotamos* $\mathrm{ord}_b(a)$, *como sendo o menor inteiro positivo u satisfazendo* $a^u \equiv 1 \pmod{b}$.

Teorema 1.25. *Seja n um inteiro positivo com* $\mathrm{mdc}(n,q) = 1$. *Então $\Phi_n(x)$ se fatora em $\varphi(n)/s$ polinômios mônicos irredutíveis sobre $\mathbb{F}_q$, todos de grau $s = \mathrm{ord}_n(q)$.*

Demonstração. Veja [8, Theorem 2.47]. □

Uma propriedade importante sobre os polinômios ciclotômicos é que, sob certas condições, vale $\Phi_{mp^t}(x) = \Phi_{mp}(x^{p^{t-1}})$. Para provar esse resultado vamos precisar de algumas propriedades da função totiente de Euler.

Lema 1.26. *Sejam n, m e k inteiros positivos com* $\mathrm{mdc}(n,m) = 1$ *e p um número primo. Então*

(i) $\varphi(mn) = \varphi(n)\varphi(m)$;

(ii) $\varphi(p^k) = p^k\left(1 - \dfrac{1}{p}\right)$.

Demonstração. Veja [11, Teoremas 4.3 e 4.4]. □

No que segue, utilizaremos $\partial(f(x))$ para denotar o grau do polinômio $f(x)$.

Lema 1.27. *Sejam m, p e t inteiros positivos, tais que* $\mathrm{mdc}(mp,q) = 1$. *Então a seguinte igualdade vale em $\mathbb{F}_q[x]$:*

$$\Phi_{mp^t}(x) = \Phi_{mp}(x^{p^{t-1}}), \tag{1.2}$$

Demonstração. Vamos mostrar inicialmente que, se $p \mid m$, então

$$\Phi_{mp}(x) = \Phi_m(x^p). \tag{1.3}$$

Podemos escrever $m = p^r n$, em que $r \geq 0$ e $p \nmid n$. Pelas propriedades do lema anterior, temos

$$\partial(\Phi_{mp}(x)) = \varphi(mp) = \varphi(p^{r+1}n) = \varphi(p^{r+1})\varphi(n) = p^{r+1}(1 - 1/p)\varphi(n),$$

e também

$$\partial(\Phi_m(x^p)) = p\partial(\Phi_m(x)) = p\varphi(m) = p\varphi(p^r n) = pp^r(1 - 1/p)\varphi(n) = p^{r+1}(1 - 1/p)\varphi(n).$$

Assim, os polinômios em (1.3) têm o mesmo grau $\varphi(mp)$, logo, o mesmo número de raízes. Esses polinômios são mônicos, para provar a igualdade basta provar que eles possuem as mesmas

raízes. Nesse caso, é suficiente provar que toda raiz de $\Phi_{mp}(x)$ também é raiz de $\Phi_m(x^p)$. Seja ω uma raiz de $\Phi_{mp}(x)$, isto é, uma mp-ésima raiz primitiva da unidade. Então $\text{ord}(\omega) = mp$ e $\text{ord}(\omega^p) = m$. Note que α é uma raiz de $\Phi_m(x^p)$ se, e somente se α^p é uma m-ésima raiz primitiva da unidade, isto é, $\text{ord}(\alpha^p) = m$. Dessa forma, ω é uma raiz de $\Phi_m(x^p)$. Ou seja, cada mp-ésima raiz primitiva da unidade é também uma raiz de $\Phi_m(x^p)$.

Vamos provar (1.2) por indução sobre t. O caso $t = 1$ é imediato. Suponha que vale para um certo $t > 1$, isto é, $\Phi_{mp^t}(x) = \Phi_{mp}(x^{p^{t-1}})$. Assim, pela Equação (1.3) e pela hipótese de indução, temos

$$\Phi_{mp^{t+1}}(x) = \Phi_{mp^tp}(x) = \Phi_{mp^t}(x^p) = \Phi_{mp}((x^p)^{p^{t-1}}) = \Phi_{mp}(x^{p^t}).$$

Donde $\Phi_{mp^{t+1}}(x) = \Phi_{mp}(x^{p^{(t+1)-1}})$ e o resultado está provado. □

Agora que vimos alguns resultados importantes, vamos apresentar alguns polinômios ciclotômicos que serão utilizados no Capítulo 4. Para isso, vamos usar o SageMath, cuja documentação pode ser encontrada em [12].

Definição 1.28. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio com grau positivo. Se existem polinômios $f_1(x), \ldots, f_r(x) \in \mathbb{F}_q[x]$, mônicos e irredutíveis sobre $\mathbb{F}_q$ e $a \in \mathbb{F}_q^*$, tais que $f(x) = af_1(x) \ldots f_r(x)$, então dizemos que essa é a fatoração de $f(x)$ sobre $\mathbb{F}_q$. Essa expressão é única, a menos da ordem dos fatores.*

Exemplo 1.29. *Pelo Exemplo 1.10, $\mathbb{F}_2$ é o subcorpo primo de $\mathbb{F}_4$. Pelo item (ii) do Teorema 1.23, o polinômio $\Phi_3(x)$ é o mesmo sobre $\mathbb{F}_2$ e $\mathbb{F}_4$. Vamos calcular esse polinômio. O código para fazer isso no SageMath é o seguinte*

```
1. sage: F = GF(2)
2. sage: R.<x> = PolynomialRing(F)
3. sage: f = R.cyclotomic_polynomial(3)
4. sage: f
5. x^2+x+1
```

Na primeira linha é definido o corpo $F = \mathbb{F}_2$. Na sequência definimos o anel de polinômios $R = \mathbb{F}_2[x]$. Na terceira linha definimos $f = \Phi_3(x)$ nesse anel de polinômios e na quarta linha utilizamos um comando para exibir tal polinômio. Como resposta, obtemos a quinta linha, ou seja, $\Phi_3(x) = x^2 + x + 1$. Para fatorar esse polinômio basta utilizar o comando "f.factor()":

```
6. sage: f.factor()
7. x^2+x+1
```

O programa então nos mostra que a fatoração desse polinômio sobre $\mathbb{F}_2$ é $x^2 + x + 1$, ou seja, ele é irredutível sobre $\mathbb{F}_2$, como já vimos no Exemplos 1.10. No entanto, esse polinômio é redutível sobre $\mathbb{F}_4$. Para ver isso, adaptamos o código para

```
1. sage F.<alpha> = GF(4, modulus='primitive')
2. sage R.<x> = PolynomialRing(F)
3. sage f = R.cyclotomic_polynomial(3)
4. sage f.factor()
5. (x+alpha)*(x+alpha+1)
```

A diferença é que na primeira linha estamos definindo o corpo $F = \mathbb{F}_4$, que possui α como elemento primitivo. Observamos então que $\Phi_3(x)$ se fatora sobre $\mathbb{F}_4$ como $\Phi_3(x) = (x-\alpha)(x-\alpha^2)$, já que $\alpha^2 = \alpha + 1$.

Exemplo 1.30. *Fazendo as adaptações necessárias no código apresentado no exemplo anterior, podemos calcular as seguintes fatorações sobre $\mathbb{F}_2$*

(i) $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$;

(ii) $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x^2 + 1)(x^3 + x + 1)$;

(iii) $\Phi_{21}(x) = x^{12}+x^{11}+x^9+x^8+x^6+x^4+x^3+x+1 = (x^6+x^4+x^2+x+1)(x^6+x^5+x^4+x^2+1)$.

Exemplo 1.31. *Sobre $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, temos as seguintes fatorações*

(i) $\Phi_3(x) = x^2 + x + 1 = (x + \alpha)(x + \alpha^2)$;

(ii) $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = (x^2 + \alpha x + 1)(x^2 + \alpha^2 x + 1)$;

(iii) $\Phi_{15}(x) = \prod_{i=1}^{2}(x^2 + x + \alpha^i)(x^2 + \alpha^i x + \alpha^i)$;

(iv) $\Phi_{21}(x) = \prod_{i=1}^{2}(x^3 + \alpha^i x + 1)(x^3 + \alpha^i x^2 + 1)$;

(v) $\Phi_{35}(x) = (x^6 + \alpha x^4 + \alpha x^3 + x^2 + \alpha^2 x + 1)(x^6 + \alpha^2 x^4 + \alpha^2 x^3 + x^2 + \alpha x + 1)(x^6 + \alpha x^5 + x^4 + \alpha^2 x^3 + \alpha^2 x^2 + 1)(x^6 + \alpha^2 x^5 + x^4 + \alpha x^3 + \alpha x^2 + 1)$;

(vi) $\Phi_{63}(x) = (x^3 + x^2 + x + \alpha)(x^3 + x^2 + x + \alpha^2)(x^3 + x^2 + \alpha x + \alpha^2)(x^3 + x^2 + \alpha^2 x + \alpha)(x^3 + \alpha x^2 + x + \alpha^2)(x^3 + \alpha x^2 + \alpha x + \alpha)(x^3 + \alpha x^2 + \alpha^2 x + \alpha)(x^3 + \alpha x^2 + \alpha^2 x + \alpha^2)(x^3 + \alpha^2 x^2 + x + \alpha)(x^3 + \alpha^2 x^2 + \alpha x + \alpha)(x^3 + \alpha^2 x^2 + \alpha x + \alpha^2)(x^3 + \alpha^2 x^2 + \alpha^2 x + \alpha^2)$.

1.3 Polinômios

1.3.1 Raízes de Polinômios Irredutíveis

Definição 1.32. *Seja β uma raiz do polinômio $f(x) \in \mathbb{F}_q[x]$. Definimos a multiplicidade de β como sendo o maior inteiro positivo k, tal que $(x-\beta)^k$ divide $f(x)$. Se $k = 1$, dizemos que β é uma raiz simples de $f(x)$, caso contrário, dizemos que é uma raiz múltipla de $f(x)$.*

Teorema 1.33. *Um elemento β é uma raiz múltipla de $f(x) \in F[x]$ se, e somente se é raiz de $f(x)$ e de $f'(x)$.*

Teorema 1.34. *Seja $f(x)$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então $f(x)$ tem uma raiz α em $\mathbb{F}_{q^m}$. Além disso, todas as raízes de $f(x)$ são simples e dadas pelos elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^m-1}$ de $\mathbb{F}_{q^m}$.*

Demonstração. Veja [8, Theorem 2.14]. □

Corolário 1.35. *Seja $f(x)$ um polinômio de grau m irredutível sobre $\mathbb{F}_q$. Então o corpo de decomposição de $f(x)$ sobre $\mathbb{F}_q$ é $\mathbb{F}_{q^m}$.*

Demonstração. Veja [8, Corollary 2.15]. □

Definição 1.36. *Sejam $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e $\alpha \in \mathbb{F}_{q^m}$. Os elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^m-1}$ de $\mathbb{F}_{q^m}$ são chamados de conjugados de α com respeito a $\mathbb{F}_q$.*

Teorema 1.37. *Os distintos automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são exatamente os mapas*

$$\sigma_j \colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m},$$

definidos por $\sigma_j(x) = x^{q^j}$, para $0 \leq j \leq m-1$.

Demonstração. Veja [8, Theorem 2.21]. □

1.3.2 Ordem de polinômios

Lema 1.38. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio de grau $m \geq 1$ com $f(0) \neq 0$. Então existe um inteiro positivo $e \leq q^m - 1$, tal que $f(x)$ divide $x^e - 1$.*

Demonstração. Veja [8, Lemma 3.1]. □

Definição 1.39. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio não nulo. Se $f(0) \neq 0$, então o menor inteiro positivo e para o qual $f(x)$ divide $x^e - 1$ é chamado de ordem de $f(x)$ e denotado por $\operatorname{ord}(f(x))$. Se $f(0) = 0$, então $f(x) = x^r g(x)$, em que o inteiro positivo r e $g(x) \in \mathbb{F}_q[x]$, com $g(0) \neq 0$, são unicamente determinados; definimos então $\operatorname{ord}(f(x)) = \operatorname{ord}(g(x))$.*

A ordem de um polinômio também pode ser chamada de período ou de expoente. A ordem de um polinômios irredutível pode ser caracterizada da seguinte maneira.

Teorema 1.40. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m com $f(0) \neq 0$. Então $\operatorname{ord}(f(x))$ é igual a ordem de qualquer raiz de $f(x)$ no grupo multiplicativo $\mathbb{F}_{q^m}^*$.*

Demonstração. Veja [8, Theorem 3.3]. □

Exemplo 1.41. *Se $d \geq 1$ é um inteiro ímpar e $\Phi_d(x) \in \mathbb{F}_q[x]$, em que q é uma potência de 2, então $\operatorname{ord}(\Phi_d(x)) = d$. De fato, como $x^d - 1 = \prod_{\ell \mid d} \Phi_\ell(x)$, é claro que $\Phi_d(x)$ divide $x^d - 1$. Para $n < d$, os únicos polinômios ciclotômicos que dividem $x^n - 1$ são $\Phi_\ell(x)$, em que $\ell \mid n$. Como $n < d$, segue que $d \nmid n$ e, consequentemente, $\Phi_d(x)$ não divide $x^n - 1$. Portanto, $\operatorname{ord}(\Phi_d(x)) = d$.*

Exemplo 1.42. *Se $p > 1$ é um primo qualquer, então a ordem de qualquer fator irredutível de $\Phi_p(x)$ sobre $\mathbb{F}_q[x]$ é p, em que q é uma potência de 2. De fato, pelo exemplo anterior,* $\mathrm{ord}(\Phi_p(x)) = p$. *Por definição, as raízes de qualquer fator irredutível de $\Phi_p(x)$ são p-ésimas raízes primitivas da unidade, que têm ordem p. O resultado segue pelo Teorema 1.40.*

1.3.3 Polinômios Irredutíveis

Definição 1.43. *Para qualquer inteiro $n > 1$,* $\mathrm{rad}(n)$ *denota o radical de n, isto é, o produto dos distintos fatores primos de n, isto é, se $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ é a fatoração de n, então* $\mathrm{rad}(n) = p_1 \dots p_r$.

Teorema 1.44. *Sejam n um inteiro positivo e $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau m e ordem e. Então o polinômio $f(x^n)$ é irredutível sobre $\mathbb{F}_q$ somente se as seguintes condições são satisfeitas*

(i) $\mathrm{rad}(n)$ *divide e;*

(ii) $\mathrm{mdc}(n, (q^m - 1)/e) = 1$;

(iii) se 4 divide n, então 4 divide $q^m - 1$.

Além disso, se $f(x^n)$ é irredutível, então ele tem grau mn e ordem en.

Demonstração. Veja [8, Theorem 3.35]. □

Vamos utilizar o teorema anterior para provar que alguns polinômios são irredutíveis, já conhecendo a irredutibilidade de outros.

Exemplo 1.45. *Para qualquer inteiro positivo k, o polinômio $\Phi_{3^k}(x)$ é irredutível sobre $\mathbb{F}_2$. De fato, pelo Lema 1.27, temos $\Phi_{3^k}(x) = \Phi_3(x^{3^{k-1}})$. Também já vimos que $\Phi_3(x)$ é irredutível de grau 2 e ordem 3 sobre $\mathbb{F}_2$. Além disso, note que* $\mathrm{rad}(3^{k-1}) = 3$ *divide* 3 *e* $\mathrm{mdc}(3^{k-1}, (2^2-1)/3) = \mathrm{mdc}(3^{k-1}, 1) = 1$. *Pelo teorema anterior, isso implica que $\Phi_{3^k}(x)$ é irredutível sobre $\mathbb{F}_2$, possui grau $2 \cdot 3^{k-1}$ e ordem $3 \cdot 3^{k-1}$.*

Exemplo 1.46. *Os polinômios $(x^{3 \cdot 7^{k-1}} + x^{2 \cdot 7^{k-1}} + 1)$ e $(x^{3 \cdot 7^{k-1}} + x^{7^{k-1}} + 1)$ são irredutíveis sobre $\mathbb{F}_2$. De fato, já mostramos que $\Phi_7(x) = (x^3 + x^2 + 1)(x^3 + x + 1)$, em que $(x^3 + x^2 + 1)$ e $(x^3 + x + 1)$ são irredutíveis sobre $\mathbb{F}_2$. O resultado segue fazendo uma análise similar à que foi feita no exemplo anterior e utilizando o Teorema 1.44.*

Exemplo 1.47. *Utilizando as fatorações dos polinômios ciclotômicos que já calculamos e fazendo uma análise similar à que foi feita nos dois exemplos anteriores é possível provar que os seguintes polinômios são irredutíveis sobre $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$:*

(i) $x^{3^{k-1}} + \alpha^i$, *para* $i \in \{1, 2\}$;

(ii) $x^{2 \cdot 5^{k-1}} + \alpha^i x^{5^{k-1}} + 1$, *para* $i \in \{1, 2\}$;

(iii) $x^{2 \cdot 3^{m-1} \cdot 5^{k-1}} + x^{3^{m-1} \cdot 5^{k-1}} + \alpha^i$ *e* $x^{2 \cdot 3^{m-1} \cdot 5^{k-1}} + \alpha^i x^{3^{m-1} \cdot 5^{k-1}} + \alpha^i$, *para* $i \in \{1, 2\}$;

(iv) $x^{3\cdot 7^{k-1}} + \alpha^i x^{2\cdot 7^{k-1}} + 1$ *e* $x^{3\cdot 7^{k-1}} + \alpha^i x^{7^{k-1}} + 1$, *para* $i \in \{1, 2\}$.

A irredutibilidade desses polinômios será essencial para a classificação dos pares 3-sparse que faremos no Capítulo 4.

Capítulo 2

Números p-ádicos

2.1 A construção de $\mathbb{Q}_p$

Neste capítulo, fixamos p como um número primo. A construção do corpo dos números p-ádicos que apresentaremos aqui é feita por meio de sequências de Cauchy e para fazê-la precisamos de algumas definições.

Definição 2.1. *Um valor absoluto sobre um corpo F é uma função*

$$|\cdot| : F \to [0, \infty)$$

com as seguintes propriedades:

(i) $|x| = 0$ *se, e somente se,* $x = 0$*;*

(ii) $|x \cdot y| = |x| \cdot |y|$*, para todo* $x, y \in F$*;*

(iii) $|x + y| \leq |x| + |y|$*, para todo* $x, y \in F$*.*

Um valor absoluto sobre F é "não-arquimediano" se tem a seguinte propriedade:

(iv) $|x + y| \leq \max\{|x|, |y|\}$.

Caso contrário, o valor absoluto é dito arquimediano. Observamos ainda que a propriedade (iv) implica a (iii).

Alguns exemplos de valor absoluto são os seguintes.

Exemplo 2.2. *A função $|\cdot| : F \to [0, \infty)$, definida por*

$$|x| = \begin{cases} 1, & \text{se } x \neq 0 \\ 0, & \text{se } x = 0, \end{cases}$$

é o valor absoluto trivial em F. É fácil ver que esse valor absoluto é não-arquimediano.

Exemplo 2.3. *A função* $|\cdot|_\infty : \mathbb{Q} \to [0, \infty)$*, definida por*

$$|x|_\infty = \begin{cases} x, \ \textit{se } x \geq 0 \\ -x, \ \textit{se } x < 0, \end{cases}$$

é o valor absoluto usual em $\mathbb{Q}$*. Tomando* $x = y = 1$*, é fácil ver que esse valor absoluto é arquimediano.*

Definição 2.4. *Sejam* $\mathbb{Q}$ *munido com um valor absoluto* $|\cdot|$ *e* $(a_n)_n$ *uma sequência de números racionais.*

- *Dizemos que essa sequência é de Cauchy com respeito a* $|\cdot|$ *se para todo* $\epsilon > 0$*, existe um* $n_0 \in \mathbb{N}$*, tal que* $|a_n - a_m| < \epsilon$ *sempre que* $n, m \geq n_0$*.*
- *Dizemos que essa sequência converge para* $a \in \mathbb{Q}$ *com respeito a* $|\cdot|$ *se para todo* $\epsilon > 0$*, existe um* $n_0 \in \mathbb{N}$*, tal que* $|a_n - a| < \epsilon$ *sempre que* $n \geq n_0$*.*

Agora vamos definir o valor absoluto p-ádico, para tanto, precisamos do conceito de valorização p-ádica, que "mede" quantas vezes p divide um número inteiro.

Definição 2.5. *Seja* $a \in \mathbb{Q}, a \neq 0$ *. Definimos a valorização p-ádica de a como sendo o inteiro* $v_p(a)$ *definido pela condição*

$$a = p^{v_p(a)} \frac{c}{b}, \ \textit{em que } c, b \in \mathbb{Z} \ \textit{e } p \nmid cb.$$

Convencionamos que $v_p(0) = \infty$*.*

Se $a, b \in \mathbb{Q}$, então $ab = p^{v_p(a)} a' p^{v_p(b)} b' = p^{v_p(a)+v_p(b)} a'b'$, em que $p \nmid a', b'$ e, consequentemente, $p \nmid a'b'$. Logo, $v_p(ab) = v_p(a) + v_p(b)$.

Exemplo 2.6. *Vamos calcular algumas valorizações.*

(i) $35 = 5 \cdot 7 \implies v_5(35) = v_7(35) = 1$*;*

(ii) Para qualquer inteiro k*, é claro que* $v_2(2k + 1) = 0$*, já que* $2k + 1$ *é ímpar;*

(iii) $\dfrac{7}{12} = 2^{-2} \cdot \dfrac{7}{3} \implies v_2\left(\dfrac{7}{12}\right) = -2$

(iv) $\dfrac{123}{48} = 3^0 \cdot \dfrac{41}{16} \implies v_3\left(\dfrac{123}{48}\right) = 0.$

Agora podemos definir o valor absoluto p-ádico e, na sequência, construir $\mathbb{Q}_p$.

Definição 2.7. *A função* $|.|_p : \mathbb{Q} \to [0, \infty)$*, definida por*

$$|x|_p = \begin{cases} p^{-v_p(x)}, \ \textit{se } x \neq 0 \\ 0, \ \textit{se } x = 0, \end{cases}$$

é o valor absoluto p-ádico.

Proposição 2.8. *A função $|.|_p$ é um valor absoluto não-arquimediano em $\mathbb{Q}$.*

Demonstração. Veja [5, p. 2]. □

Definição 2.9. *Considere $\mathbb{Q}$ munido com o valor absoluto p-ádico. Definimos*

$$\mathcal{C} = \{(a_n)_n \subset \mathbb{Q}; (a_n)_n \text{é uma sequência de Cauchy com respeito a } |.|_p\},$$
$$\mathcal{N} = \{(a_n)_n \in \mathcal{C}; (a_n)_n \text{ converge para } 0 \text{ com respeito a } |.|_p\}.$$

Teorema 2.10. *O conjunto $\mathcal{C}$ definido acima é um anel e $\mathcal{N}$ é um ideal maximal de $\mathcal{C}$. Consequentemente, o quociente $\mathcal{C}/\mathcal{N}$ é um corpo.*

Demonstração. Veja [6, Lemma 3.2.8]. □

Definição 2.11. *Considere $\mathbb{Q}$ munido com o valor absoluto $|.|_p$. Definimos o corpo dos números p-ádicos como sendo*

$$\mathbb{Q}_p = \mathcal{C}/\mathcal{N}.$$

Notamos que $\mathbb{Q}$ pode ser identificado em $\mathbb{Q}_p$ por meio das sequências constantes.

2.2 Algumas Propriedades em $\mathbb{Q}_p$

A primeira propriedade nos dá a possibilidade de estender o valor absoluto p-ádico definido em $\mathbb{Q}$ para $\mathbb{Q}_p$.

Lema 2.12. *Seja $(a_n)_n \in \mathcal{C}, (a_n)_n \notin \mathcal{N}$. Então a sequência de números reais $(|a_n|_p)_n$ é eventualmente estacionária, isto é, existe $n_0 \in \mathbb{N}$, tal que $|a_n|_p = |a_m|_p$, sempre que $n, m \geq n_0$.*

Demonstração. Veja [6, Lemma 3.2.10]. □

Por esse lema, se $a \in \mathbb{Q}_p, a \neq 0$ e $(a_n)_n \subset \mathbb{Q}$ é qualquer representante da classe a, então existe $n_0 \in \mathbb{N}$, tal que $\lim_{n\to\infty} |a_n|_p = |a_{n_0}|_p = p^{-v_p(a_{n_0})}$.

Definição 2.13. *Se $a \in \mathbb{Q}_p, a \neq 0$ e $(a_n)_n \subset \mathbb{Q}$ é qualquer representante da classe a, definimos*

$$|a|_p = \lim_{n\to\infty} |a_n|_p = |a_{n_0}|_p = p^{-v_p(a_{n_0})},$$

para $n_0 \in \mathbb{N}$ suficientemente grande.

Uma relação entre $\mathbb{Q}$ e $\mathbb{Q}_p$ é dada na proposição a seguir.

Definição 2.14. *Sejam A e B dois conjuntos, com $A \subset B$. Dizemos que A é um subconjunto denso de B se para todo elemento $b \in B$, existe uma sequência $(a_n)_n$ em A, tal que $b = \lim_{n\to\infty} a_n$.*

Proposição 2.15. *A imagem de $\mathbb{Q}$ pela inclusão é um subconjunto denso de $\mathbb{Q}_p$.*

Demonstração. Veja [6, Proposition 3.2.12]. □

Uma propriedade importante que $\mathbb{Q}_p$ possui é a completude.

Definição 2.16. *Dizemos que um corpo F é completo se toda sequência de Cauchy com elementos em F converge para um elemento de F.*

Teorema 2.17. *O corpo dos números p-ádicos $\mathbb{Q}_p$ é completo.*

Demonstração. Veja [6, Problem 88]. □

Agora estendemos a valorização p-ádica para elementos de $\mathbb{Q}_p$.

Lema 2.18. *Para cada $a \in \mathbb{Q}_p, a \neq 0$, existe um inteiro n, tal que $v_p(a) = n$.*

Demonstração. Pelo teorema anterior, existe uma sequência $(a_n) \subset \mathbb{Q}$, tal que $a = \lim_{n\to\infty} a_n$. Assim, $|a|_p = \lim_{n\to\infty} |a_n|_p = |a_{n_0}|_p = p^{-v_p(a_{n_0})}$, para $n_0 \in \mathbb{N}$ suficientemente grande. Ou seja, $v_p(a) = v_p(a_{n_0})$. □

Teorema 2.19. *Para todo $a \in \mathbb{Q}_p$ satisfazendo $|a|_p \leq 1$, existe uma única sequência de Cauchy $(a_n)_n$ representante de a, tal que*

(i) $0 \leq a_n < p^n$, *para* $n \in \{1, 2, 3, \dots\}$;

(ii) $a_n \equiv a_{n+1} \pmod{p^n}$, *para* $n \in \{1, 2, 3, \dots\}$.

Demonstração. Veja [5, p. 11]. □

Para $a \in \mathbb{Q}_p, |a|_p \leq 1$, é conveniente escrever cada a_n na base p, da seguinte forma:

$$a_n = b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1},$$

em que $b_j \in \{0, 1, \dots, p-1\}$, para todo $j \in \{0, 1, \dots, n-1\}$. Além disso, $a_n \equiv a_{n+1} \pmod{p^n}$ significa que

$$a_{n+1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1} + b_n p^n,$$

com $b_n \in \{0, 1, \dots, p-1\}$. De forma intuitiva, podemos pensar em a como a seguinte série

$$a = b_0 + b_1 p + \cdots + b_{n-1} p^{n-1} + b_n p^n + \cdots$$

Na verdade, essa série realmente converge para a, como veremos a seguir.

Definição 2.20. *Definimos o anel dos inteiros p-ádicos como sendo*

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p; |a|_p \leq 1\}.$$

Notamos que $\mathbb{Z}_p$ é precisamente a bola unitária fechada de $\mathbb{Q}_p$.

Lema 2.21. *Dado $a \in \mathbb{Z}_p$, a série obtida como nos comentários anteriores converge para a.*

Demonstração. Veja [6, Corollary 3.3.11]. □

Isso pode ser estendido para todos os elementos de $\mathbb{Q}_p$.

Corolário 2.22. *Todo elemento $a \in \mathbb{Q}_p$ pode ser escrito na forma*

$$a = b_{-n_0}p^{-n_0} + \cdots + b_0 + b_1 p + \cdots + b_n p^n + \cdots,$$

em que $0 \leq b_n \leq p-1$, para todo $n \geq n_0$ e $-n_0 = v_p(a)$. Essa representação é única e chamada de expansão p-ádica de a.

Demonstração. Veja [6, Corollary 3.3.12]. □

Exemplo 2.23. *Em $\mathbb{Q}_3$, temos as seguintes expansões 3-ádicas para alguns números inteiros e racionais:*

(i) $36 = 1 \cdot 3^2 + 1 \cdot 3^3$

(ii) $\dfrac{1}{36} = 1 \cdot 3^{-2} + 2 \cdot 3^{-1} + 0 \cdot 3^0 + 2 \cdot 3^1 + 0 \cdot 3^2 + 2 \cdot 3^3 + \cdots$

(iii) $-5 = 1 \cdot 3^0 + 1 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots$

(iv) $\dfrac{1}{4} = 1 \cdot 3^0 + 2 \cdot 3 + 0 \cdot 3^2 + 2 \cdot 3^3 + 0 \cdot 3^4 + 2 \cdot 3^5 + \cdots$

Também podemos considerar congruência modular no anel dos inteiros p-ádicos:

Definição 2.24. *Dados $a, b \in \mathbb{Z}_p$, dizemos que a é congruente a b módulo p, e escrevemos $a \equiv b \pmod{p}$, se $a = dp + b$, para algum $d \in \mathbb{Z}_p$.*

Lema 2.25. *O conjunto das unidades p-ádicas é dado por*

$$\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p; |a|_p = 1\} = \{a \in \mathbb{Z}_p; a \not\equiv 0 \pmod{p}\}.$$

Demonstração. Seja $a \in \mathbb{Z}_p^*$. Temos $|a|_p \leq 1$ e

$$a \in \mathbb{Z}_p^* \iff a^{-1} \in \mathbb{Z}_p^* \iff \left|a^{-1}\right|_p = |a|_p^{-1} \leq 1 \iff |a|_p \geq 1.$$

Logo, $a \in \mathbb{Z}_p^*$ se, e somente se, $|a|_p = 1$. Para a segunda igualdade:

$$|a|_p = 1 \iff a^{-v_p(a)} = 1 \iff v_p(a) = 0 \iff a \not\equiv 0 \pmod{p}.$$

□

Neste trabalho escrevemos $\pmod{p}$ no contexto dos inteiros p-ádicos, como feito acima, e também no contexto dos inteiros "convencionais". A diferenciação dessa escrita é feita pelo contexto.

Lema 2.26. *O anel dos inteiros p-ádicos é completo.*

Demonstração. Pelo Teorema 2.17, $\mathbb{Q}_p$ é completo. Além disso, $\mathbb{Z}_p$ é fechado por definição. Segue, portanto, que $\mathbb{Z}_p$ é completo. □

Podemos usar essa completude para provar o seguinte resultado, que será importante no Capítulo 3.

Lema 2.27. *Sejam $a \in \mathbb{Z}_p$ e $(b_n)_n \subset \mathbb{Z}_p$ uma sequência de Cauchy, tal que $a \equiv b_n^2 \pmod{p^n}$, para todo $n \in \mathbb{N}$. Então $a = b^2$, em que b é o limite da sequência $(b_n)_n$.*

Demonstração. Iniciamos a demonstração provando que a função $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$, definida por $f(x) = x^2$, é contínua com respeito ao valor absoluto p-ádico, isto é, se $c \in \mathbb{Q}_p$, então para todo $\epsilon > 0$, existe um $\delta > 0$, tal que $|f(x) - f(c)|_p < \epsilon$, sempre que $|x - c|_p < \delta$. Sejam então $c \in \mathbb{Q}_p$ e $\epsilon > 0$. Se $c = 0$, tomamos $\delta = \sqrt{\epsilon}$. Dessa forma,

$$|x - c|_p = |x|_p < \delta \implies |f(x) - f(c)|_p = \left|x^2\right|_p = |x|_p^2 < \delta^2 = \epsilon.$$

Para $c \neq 0$, definimos $\delta = \min\{\epsilon / |2c|_p, |2c|_p\}$. Assim, se $|x - c|_p < \delta$, temos

$$|x - c|_p < \epsilon / |2c|_p \quad \text{e} \quad |x + c|_p = |(x - c) + 2c|_p \leq \max\{|x - c|_p, |2c|_p\} \leq |2c|_p.$$

Com isso,

$$|f(x) - f(c)|_p = \left|x^2 - c^2\right|_p = |(x - c)(x + c)|_p = |x - c|_p \, |x + c|_p < \epsilon / |2c|_p \cdot |2c|_p = \epsilon.$$

Isso prova a continuidade de f. Além disso, como $\mathbb{Q}_p$ é um espaço métrico com a métrica induzida pelo valor absoluto p-ádico, vale que, se $(x_n)_n$ é uma sequência que converge para x_0 e f é uma função contínua, então $(f(x_n))_n$ converge para $f(x_0)$ (veja [9, p. 125]).

Agora provaremos o resultado. Pelo lema anterior, existe $b \in \mathbb{Z}_p$, tal que $b = \lim_{n\to\infty} b_n$. Além disso, a função x^2 é contínua, logo $\lim_{n\to\infty} b_n^2 = b^2$. Para cada $n \in \mathbb{N}$, temos $a \equiv b_n^2 \pmod{p^n}$, o que implica $|a - b_n^2|_p \leq p^{-n}$. Assim, $\lim_{n\to\infty} |a - b_n^2|_p = 0$, ou ainda, $\lim_{n\to\infty} b_n^2 = a$. Pela unicidade do limite em espaços métricos, concluímos que $a = b^2$. □

2.3 O Lema de Hensel

Uma das propriedades mais importantes no estudo dos números p-ádicos é o Lema de Hensel, que nos dá condições para verificar se um polinômio tem raízes em $\mathbb{Z}_p$.

Teorema 2.28 (Lema de Hensel)**.** *Seja $f(x)$ um polinômio com coeficientes em $\mathbb{Z}_p$. Suponha que existe $a_0 \in \mathbb{Z}_p$ satisfazendo*

$$f(a_0) \equiv 0 \pmod{p} \quad e \quad f'(a_0) \not\equiv 0 \pmod{p}.$$

Então existe um único $a \in \mathbb{Z}_p$, tal que

$$f(a) = 0 \quad e \quad a \equiv a_0 \pmod{p}.$$

Demonstração. Veja [6, Theorem 3.4.1].

□

Vejamos uma aplicação para esse lema.

Corolário 2.29. *Sejam $p \neq 2$ um número primo e $b \in \mathbb{Z}_p^*$ uma unidade p-ádica. Se existe $a_1 \in \mathbb{Z}_p$ tal que $a_1^2 \equiv b \pmod{p}$ então existe $a \in \mathbb{Z}_p^*$ tal que $a^2 = b$.*

Demonstração. Considere o polinômio $f(x) = x^2 - b$. É claro que $f(a_1) \equiv 0 \pmod{p}$. Além disso,

$$b \in \mathbb{Z}_p^* \implies |b|_p = 1 \implies |a_1|_p^2 = 1 \implies |a_1|_p = 1 \implies a_1 \in \mathbb{Z}_p^*.$$

Sendo assim, p não divide a_1. Daí, p não divide $2a_1 = f'(a_1)$. Isso implica que $f'(a_1) \not\equiv 0 \pmod{p}$. Pelo Lema de Hensel, existe $a \in \mathbb{Z}_p$, tal que $a^2 = b$ e $a \equiv a_1 \pmod{p}$. Se $a \notin \mathbb{Z}_p^*$, então p divide a. Disso, $a_1 \equiv a \equiv 0 \pmod{p}$. O que implica $b \notin \mathbb{Z}_p^*$, o que é uma contradição. Portanto, $a \in \mathbb{Z}_p^*$ e segue o resultado. □

Para finalizar a seção, apresentaremos algo mais geral que o Lema de Hensel. Para isso, interpretamos esse lema da seguinte forma: se $a_0 \in \mathbb{Z}_p$ é tal que $(x - a_0)$ é um fator de $f(x)$ módulo p, então existe $a \in \mathbb{Z}_p$, tal que $a \equiv a_0 \pmod{p}$ e $(x - a)$ é um fator de $f(x)$. Veja que isso é um caso particular do próximo teorema.

Definição 2.30. *Sejam $f(x), g(x) \in \mathbb{Z}_p$. Considere $\bar{f}(x), \bar{g}(x) \in \mathbb{F}_p[x]$ os polinômios obtidos a partir da redução dos coeficientes de $f(x)$ e $g(x)$ módulo p, respectivamente. Dizemos que $f(x)$ e $g(x)$ são relativamente primos módulo p se $\mathrm{mdc}(\bar{g}(x), \bar{h}(x)) = 1$ em $\mathbb{F}_p$, ou, equivalentemente, se existem polinômios $a(x), b(x) \in \mathbb{Z}_p[x]$, tais que*

$$a(x)g(x) + b(x)h(x) \equiv 1 \pmod{p}.$$

Teorema 2.31 (Segunda Forma do Lema de Hensel)**.** *Seja $f(x)$ um polinômio com coeficientes em $\mathbb{Z}_p$. Suponha que existem polinômios $g_1(x)$ e $h_1(x)$ com coeficientes em $\mathbb{Z}_p$ satisfazendo*

- *$g_1(x)$ é mônico;*
- *$g_1(x)$ e $h_1(x)$ são relativamente primos módulo p;*
- *$f(x) \equiv g_1(x)h_1(x) \pmod{p}$.*

Então existem polinômios $g(x)$ e $h(x)$ com coeficientes em $\mathbb{Z}_p$ satisfazendo

- *$g(x)$ é mônico;*

- $g(x) \equiv g_1(x) \pmod{p}$ *e* $h(x) \equiv h_1(x) \pmod{p}$*;*
- $f(x) = g(x)h(x)$*.*

Demonstração. Veja [6, Theorem 3.4.6]. □

2.4 Extensões de $\mathbb{Q}_p$

Começamos a seção com uma definição importante no contexto de extensões de corpos.

Definição 2.32. *Sejam K uma extensão finita de F de grau n e $\alpha \in K$. Definimos a norma de α sobre F de duas formas equivalentes:*

(i) Considerando K um espaço vetorial sobre F, podemos definir a transformação linear $T(x) = \alpha x$, para todo $x \in K$, ou seja, a multiplicação por α. Se A_α é a matriz dessa transformação linear, definimos a norma por $\mathrm{N}_{K/F}(\alpha) = \det(A_\alpha)$.

(ii) Se $f(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0 \in F[x]$ é o polinômio minimal de α sobre F, isto é, $f(x)$ é mônico, irredutível sobre F e possui α como raiz, definimos a norma por $\mathrm{N}_{K/F}(\alpha) = (-1)^{nr}a_0^r$, em que $r = [K : F(\alpha)]$.

Mais detalhes dessa equivalência podem ser encontrados em [5, p. 60].

Teorema 2.33. *Seja K uma extensão finita de $\mathbb{Q}_p$ de grau n. Então existe um único valor absoluto $|\cdot|$ sobre K que estende o valor absoluto p-ádico definido em $\mathbb{Q}_p$, isto é, $|a| = |a|_p$, para qualquer $a \in \mathbb{Q}_p$. Para todo $\alpha \in K$, esse valor absoluto é definido por*

$$|\alpha| = \left|\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)\right|_p^{1/n}$$

Demonstração. Veja [6, Theorem 5.3.5]. □

Vejamos um exemplo.

Exemplo 2.34. *Sejam $p = 3$ e $K = \mathbb{Q}_3(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}_3\}$ uma extensão de grau 2 sobre $\mathbb{Q}_3$. Vamos calcular o valor absoluto 3-ádico de $1 + \sqrt{2}$. Não é difícil verificar que $x^2 - 2x - 1 \in \mathbb{Q}_3[x]$ é o polinômio minimal de $1 + \sqrt{2}$ sobre $\mathbb{Q}_3$. Logo, $[K : \mathbb{Q}_3(1 + \sqrt{2})] = 1$. Assim,*

$$\left|1 + \sqrt{2}\right| = \left|N_{K/\mathbb{Q}_3}(1 + \sqrt{2})\right|_3^{1/2} = \left|(-1)^2(-1)\right|_3^{1/2} = |1|_3^{1/2} = 1.$$

Pois $|1|_p = p^{-v_p(1)} = p^0 = 1$, para todo primo p.

De agora em diante vamos utilizar $|.|_p$ para denotar o valor absoluto definido no teorema anterior.

Proposição 2.35. *Sejam K uma extensão finita de $\mathbb{Q}_p$ de grau n,*

$$A = \{x \in K; |x|_p \leq 1\} \quad e \quad M = \{x \in K; |x|_p < 1\}.$$

Então A é um anel, M é o seu único ideal maximal e A/M é uma extensão finita de $\mathbb{F}_p$ de grau no máximo n. Chamamos o corpo A/M de corpo residual de K.

Demonstração. Veja [5, p. 64] □

Para qualquer $x \in \mathbb{Q}_p$, temos $|x|_p = p^{-v_p(x)}$. Aplicando a função $\log_p$ em ambos os lados, obtemos $v_p(x) = -\log_p |x|_p$. Agora utilizaremos essa igualdade para estender a valorização p-ádica para um elemento de K.

Definição 2.36. *Seja K uma extensão finita de $\mathbb{Q}_p$ de grau n. Para $\alpha \in K^*$, definimos*

$$v_p(\alpha) = -\log_p |\alpha|_p = -\log_p \left|\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)\right|_p^{1/n} = -\frac{1}{n} \log_p \left|\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)\right|_p.$$

A restrição dessa valorização para elementos de $\mathbb{Q}_p$ coincide com a definição feita anteriormente de valorização p-ádica para esse corpo.

Proposição 2.37. *Seja K uma extensão finita de $\mathbb{Q}_p$ de grau n. A valorização p-ádica definida anteriormente é um homomorfismo do grupo multiplicativo K^* no grupo aditivo $\mathbb{Q}$. Além disso, $v_p(K^*) = (1/e)\mathbb{Z}$, em que e é um divisor de n.*

Demonstração. Veja [6, Proposition 5.4.2]. □

Pela proposição anterior, temos $v_p(K^*) = (1/e)\mathbb{Z}$. Como $1/e \in (1/e)\mathbb{Z}$, segue que existe um elemento $\pi \in K^*$, tal que $v_p(\pi) = 1/e$. Elementos com essa propriedade cumprem um papel fundamental no estudo das extensões finitas de $\mathbb{Q}_p$ e são chamados de uniformizantes.

Definição 2.38. *Seja K uma extensão finita de $\mathbb{Q}_p$. O número e obtido na proposição anterior é chamado de índice de ramificação de K sobre $\mathbb{Q}_p$. Se $e = 1$, dizemos que essa extensão é não ramificada. Dizemos que ela é ramificada se $e > 1$ e totalmente ramificada se $e = n$.*

Finalizamos a seção com dois resultados que serão essenciais para o Capítulo 3.

Proposição 2.39. *Seja K uma extensão de $\mathbb{Q}_p$, tal que $n = [K : \mathbb{Q}_p]$. Então $n = ef$, em que e é o índice de ramificação e $f = [A/M : \mathbb{F}_p]$.*

Demonstração. Veja [6, Proposition 5.4.6] □

Teorema 2.40. *Para cada inteiro positivo n, existe exatamente uma extensão não ramificada e cíclica de $\mathbb{Q}_p$ de grau n. Essa extensão pode ser obtida adjuntando a $\mathbb{Q}_p$ uma $(p^n - 1)$-ésima raiz primitiva da unidade*

Demonstração. Veja [6, Proposition 5.4.11]. □

Capítulo 3

A Paridade do Número de Fatores Irredutíveis de $x^n + x^k + 1$

O objetivo principal deste capítulo é estudar alguns critérios que determinam a paridade da quantidade de fatores irredutíveis do trinômio $x^n + x^k + 1$ sobre $\mathbb{F}_2$, com base nos resultados de [13]. Para isso, iniciamos com a definição do discriminante de um polinômio e exploramos suas propriedades, destacando a relação entre o discriminante e a paridade do número de fatores irredutíveis de um polinômio sobre $\mathbb{F}_p$.

O teorema central de [13] estabelece que, para um polinômio $f(x) \in \mathbb{Z}_p$ cuja redução módulo p não possui raízes múltiplas, o número r de fatores irredutíveis de $\bar{f}(x)$ sobre $\mathbb{F}_p$ tem a mesma paridade que o grau n de $f(x)$ se, e somente se, o discriminante $D(f)$ é um quadrado em $\mathbb{Q}_p$. Esse resultado é complementado por critérios mais práticos para verificar quando $D(f)$ é um quadrado em $\mathbb{Q}_p$.

Para aplicar esses resultados aos trinômios $x^n + x^k + 1$, desenvolvemos uma fórmula explícita para o discriminante de um trinômio da forma $x^n + ax^k + b$, utilizando o conceito de resultante de polinômios. A partir dessa fórmula, demonstramos um corolário que classifica a paridade do número de fatores irredutíveis de $x^n + x^k + 1$ sobre $\mathbb{F}_2$ em função das paridades de n e k, e de congruências envolvendo n, k e o discriminante.

3.1 O discriminante

Definição 3.1. *Seja $f(x)$ um polinômio sobre um corpo F. O discriminante de $f(x)$ é dado por $D(f) = \delta(f)^2$, com*

$$\delta(f) = \prod_{\substack{i,j=1 \\ i<j}}^{n} (\alpha_i - \alpha_j),$$

em que $\alpha_1, \ldots, \alpha_n$ são as raízes de $f(x)$ (contadas com multiplicidade) em alguma extensão de F.

Exemplo 3.2. *Vamos calcular o discriminante de $f(x) = x^2 + bx + c \in F[x]$. As raízes desse*

polinômio são $\alpha_1 = \dfrac{-b+\sqrt{b^2-4c}}{2}$ *e* $\alpha_2 = \dfrac{-b-\sqrt{b^2-4c}}{2}$. *Com isso,*

$$\delta(f) = \alpha_1 - \alpha_2 = \frac{-b+\sqrt{b^2-4c}}{2} - \frac{-b-\sqrt{b^2-4c}}{2} = \frac{2\sqrt{b^2-4c}}{2} = \sqrt{b^2-4c}.$$

Logo,

$$D(f) = \delta(f)^2 = b^2 - 4c.$$

Observação 3.3. *Seja $f(x)$ um polinômio mônico com coeficientes em $\mathbb{Z}_p$. Então $\bar{f}(x)$ denotará o polinômio sobre $\mathbb{F}_p$ obtido a partir da redução dos coeficientes de $f(x)$ módulo p. Sejam $\alpha_1, \ldots, \alpha_n$ as raízes de $f(x)$ em alguma extensão de $\mathbb{Q}_p$. Assim, $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ e, portanto, $\bar{f}(x) = (x-\bar{\alpha_1})\cdots(x-\bar{\alpha_n})$. Segue então que $D(\bar{f})$ é a redução de $D(f)$ módulo p. Em particular, se $\bar{f}(x)$ não tem raízes múltiplas, então $D(\bar{f}) \neq 0$ em $\mathbb{F}_p$ e, sendo assim, $D(f)$ é primo com p.*

Exemplo 3.4. *Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}_p$. Para cada $j \in \{0, \ldots, n\}$, podemos escrever $a_j = b_{j0} + b_{j1}p + b_{j2}p^2 + \cdots$, em que $b_{jk} \in \{0, 1, \ldots, p-1\}$, para todo $k \geq 0$. Assim, a redução módulo p de cada a_j é dada por $\bar{a_j} = b_{j0} \in \mathbb{F}_p$. Logo, $\bar{f}(x) = b_{n0}x^n + b_{(n-1)0}x^{n-1} + \cdots + b_{10}x + b_{00} \in \mathbb{F}_p[x]$.*

Exemplo 3.5. *Seja $f(x) = -5x + 36 \in \mathbb{Z}_3[x]$. Utilizando o Exemplo 2.23, é fácil ver que $\bar{f}(x) = x \in \mathbb{F}_3[x]$.*

Uma forma alternativa para o discriminante que é útil em alguns momentos será apresentada no resultado a seguir.

Lema 3.6. *Seja $f(x)$ um polinômio de grau n sobre um corpo F. O discriminante de $f(x)$ é dado por*

$$D(f) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\alpha_i).$$

Demonstração. Podemos escrever $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$. Se $f(x)$ possuir alguma raiz múltipla, então $\delta(f) = 0$ e o resultado é trivial, pois raízes múltiplas de $f(x)$ também anulam a sua derivada. Suponhamos então que $f(x)$ só tem raízes simples. Sabemos que

$$f'(x) = \sum_{k=1}^{n} \prod_{\substack{i=1 \\ i\neq k}}^{n} (x-\alpha_i).$$

Observe que, para $k \neq j$, vale

$$\prod_{\substack{i=1 \\ i\neq k}}^{n} (\alpha_j - \alpha_i) = 0,$$

pois em algum momento $i = j$.

Assim, ao calcular $f'(\alpha_j)$, a única parcela que sobra no somatório é aquela em que $k = j$. Logo,

$$\prod_{j=1}^{n} f'(\alpha_j) = \prod_{j=1}^{n} \left(\sum_{k=1}^{n} \prod_{\substack{i=1 \\ i \neq k}}^{n} (\alpha_j - \alpha_i) \right) = \prod_{j=1}^{n} \prod_{\substack{i=1 \\ i \neq j}}^{n} (\alpha_j - \alpha_i) = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (\alpha_i - \alpha_j). \tag{3.1}$$

Observe agora que

$$\prod_{\substack{i,j=1 \\ i \neq j}}^{n} (\alpha_i - \alpha_j) = \prod_{\substack{i,j=1 \\ i < j}}^{n} (\alpha_i - \alpha_j)(\alpha_j - \alpha_i) = \prod_{\substack{i,j=1 \\ i < j}}^{n} (-1)(\alpha_i - \alpha_j)^2. \tag{3.2}$$

Agora, percebemos que há $\binom{n}{2} = \dfrac{n(n-1)}{2}$ pares (i, j), com $i < j$, e cada um desses pares contribui com um fator (-1) no produto anterior. Assim,

$$\begin{aligned} \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (-1)(\alpha_i - \alpha_j)^2 &= (-1)^{n(n-1)/2} \prod_{\substack{i,j=1 \\ i < j}}^{n} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{n(n-1)/2} \delta(f)^2 \\ &= (-1)^{n(n-1)/2} D(f). \end{aligned} \tag{3.3}$$

De (3.1), (3.2) e (3.3), temos

$$\prod_{j=1}^{n} f'(\alpha_j) = (-1)^{n(n-1)/2} D(f).$$

Portanto,

$$D(f) = (-1)^{n(n-1)/2} \prod_{j=1}^{n} f'(\alpha_j).$$

□

A seguir, apresentaremos o teorema principal de [13], seguido de alguns corolários que serão importantes para demonstrar o Corolário 3.17, que, por sua vez, será essencial para a classificação dos pares $(n, 2)$ que são 3-sparse.

Teorema 3.7. *Seja $f(x)$ um polinômio mônico de grau n com coeficientes em $\mathbb{Z}_p$. Assuma que $\bar{f}(x)$ não tem raízes múltiplas. Seja r o número de fatores irredutíveis de $\bar{f}(x)$ sobre $\mathbb{F}_p$. Então*

$$r \equiv n \pmod 2 \text{ se, e somente se, } D(f) \text{ é um quadrado em } \mathbb{Q}_p.$$

Demonstração. Podemos fatorar $\bar{f}(x) = \bar{f}_1(x) \cdots \bar{f}_r(x)$ sobre $\mathbb{F}_p$. Como os polinômios $\bar{f}_j(x)$ são

relativamente primos entre si para $j \in \{1, 2, \ldots, r\}$, a segunda forma do Lema de Hensel (2.31) garante que existe uma fatoração equivalente $f(x) = f_1(x) \cdots f_r(x)$ sobre $\mathbb{Q}_p$, em que $\bar{f}_j(x)$ é a redução de $f_j(x)$ módulo p. Suponhamos que existem $g_j(x), h_j(x) \in \mathbb{Q}_p[x]$, tais que $f_j(x) = g_j(x)h_j(x)$, então $\bar{f}_j(x) = \bar{g_j}(x)\bar{h_j}(x)$. Como $\bar{f}_j(x)$ é irredutível para todo $j \in \{1, 2, \ldots, r\}$, segue que $\bar{g_j}(x)$ ou $\bar{h_j}(x)$ é constante. Consequentemente, $g_j(x)$ ou $h_j(x)$ também o é, pois o grau da redução de um polinômio mônico é igual ao grau do próprio polinômio.

Seja $m = \text{mmc}(\partial(f_1(X)), \ldots, \partial(f_r(X)))$. Pelo Teorema 2.40, existe uma única extensão E_1 de Galois, cíclica e não ramificada de $\mathbb{Q}_p$, de grau m. Como essa extensão é não ramificada, a Proposição 2.39 implica que $m = [K_1 \colon \mathbb{F}_p]$, em que K_1 é o corpo residual de E_1 sobre $\mathbb{Q}_p$. Pelo Lema 1.8, K_1 é o corpo finito com p^m elementos, isto é, $\mathbb{F}_{p^m}$. Para cada $j \in \{1, 2, \ldots, r\}$, se $n_j = \partial(\bar{f}_j(x))$, então o Corolário 1.35 implica que o corpo de decomposição de $\bar{f}_j(x)$ é $\mathbb{F}_{p^{n_j}}$. Isso significa que todas as raízes de $\bar{f}_j(x)$ pertencem a $\mathbb{F}_{p^{n_j}}$, que, por sua vez, está contido em $\mathbb{F}_{p^m}$ (Teorema 1.11). Logo, $\mathbb{F}_{p^m}$ contém todas as raízes de $\bar{f}_j(x)$, para todo $j \in \{1, 2, \ldots, r\}$, sendo assim, contém todas as raízes de $\bar{f}(x)$. Disto, $\bar{f}(x)$ se fatora completamente em $\mathbb{F}_{p^m}$ e, pela segunda forma do Lema de Hensel (Teorema 2.31), $f(x)$ se fatora completamente sobre E, donde concluímos que E é o corpo de decomposição de $f(x)$ sobre $\mathbb{Q}_p$. Note que $E \subset E_1$.

Como $E_1/\mathbb{Q}_p$ é uma extensão cíclica e de Galois e $E \subset E_1$, o Teorema Fundamental da Teoria de Galois (veja [7, Chapter IV]) implica que $E/\mathbb{Q}_p$ também é cíclica. Seja σ o gerador do grupo de Galois de $E/\mathbb{Q}_p$ e β_j uma raiz de $f_j(x)$, para cada $j \in \{1, 2, \ldots, r\}$ fixo. Então as raízes de $f_j(x)$ são $\sigma^i(\beta_j)$, em que $0 \leq i < n_j$ e $n_j = \partial(f_j(x))$. Portanto, as raízes de $f(x)$ são $\sigma^i(\beta_j)$, com $j \in \{1, 2, \ldots, r\}$ e $0 \leq i < n_j$. Podemos ordená-las definindo

$$(i_1, j_1) < (i_2, j_2) \quad \text{se} \quad \begin{cases} j_1 < j_2 \\ \quad \text{ou} \\ j_1 = j_2 \text{ e } i_1 < i_2. \end{cases}$$

Além disso, para qualquer $0 \leq i < n_j$, o símbolo (i, j) será interpretado como (i', j), em que $i \equiv i' \pmod{n_j}$, $0 \leq i' < n_j$. Veja que isso faz sentido, pois para cada $j \in \{1, 2, \ldots, r\}$, de $i \equiv i' \pmod{n_j}$ segue que $i = n_j y + i'$, em que $y \in \mathbb{Z}$ e, sendo assim, $\sigma^i(\beta) = \sigma^{n_j q} \circ \sigma^{i'}(\beta) = \sigma^{i'}(\beta)$ (σ^{n_j} é a identidade pois n_j é o grau de $[\mathbb{F}_{p^{n_j}} \colon \mathbb{F}_p]$ e σ gera o grupo de Galois dessa extensão). Assim,

$$\delta(f) = \prod_{(i_1, j_1) < (i_2, j_2)} (\sigma^{i_1}(\beta_{j_1}) - \sigma^{i_2}(\beta_{j_2})).$$

Aplicando o isomorfismo σ em ambos os lados, obtemos

$$\sigma(\delta(f)) = \prod_{(i_1, j_1) < (i_2, j_2)} (\sigma^{i_1+1}(\beta_{j_1}) - \sigma^{i_2+1}(\beta_{j_2})).$$

Note que os fatores de $\delta(f)$ e $\sigma(\delta(f))$ são os mesmos, a menos, possivelmente, de troca de sinais. O termo $\sigma^{i_1+1}(\beta_{j_1}) - \sigma^{i_2+1}(\beta_{j_2})$ aparece com o mesmo sinal em ambos os casos se, e

somente se, $(i_1+1, j_1) < (i_2+1, j_2)$. Esse é o caso quando $j_1 < j_2$ ou quando $j_1 = j_2 = j$ e $i_2 < n_j - 1$. Veja que, se $j_1 = j_2 = j$ e $i_2 = n_j - 1$, então

$$(i_2+1, j) = (n_j, j) = (0, j) < (i_1+1, j).$$

Ou seja, a quantidade de termos que aparecem com sinal trocado é igual a quantidade de pares $((i_1, j), (n_j - 1, j))$, em que $0 \leq i_1 \leq n_j - 2$. Para cada $j \in \{1, 2, \ldots, r\}$ fixo, existem $n_j - 1$ desses pares, que só dependem de i_1. Como j varia entre 1 e r e a soma dos n_j resulta em n (o grau de $f(x)$), segue que existem

$$(n_1 - 1) + (n_2 - 1) + \cdots + (n_r - 1) = n_1 + n_2 + \cdots + n_r - r = n - r$$

desses pares no total.

Isso mostra que $\sigma(\delta(f)) = (-1)^{n-r}\delta(f)$. Veja que $D(f) = \delta(f)^2$ é um quadrado em $\mathbb{Q}_p$ se, e somente se, $\delta(f) \in \mathbb{Q}_p$. O que ocorre se, e somente se, $\sigma(\delta(f)) = \delta(f)$, pois $\mathbb{Q}_p$ é o corpo fixo por σ. Ou seja, se, e somente se, $n - r \equiv 0 \pmod 2$, isto é, se o expoente $n - r$ for par.

Portanto, $D(f)$ é um quadrado em $\mathbb{Q}_p$ se, e somente se, $n \equiv r \pmod 2$. □

Lema 3.8. *Seja a um inteiro p-ádico primo com p. Então a é um quadrado p-ádico se, e somente se, a é um quadrado módulo $4p$.*

Demonstração. Por um lado, suponhamos que existe $b \in \mathbb{Z}_p$, tal que $a = b^2$. Então é claro que $a \equiv b^2 \pmod{4p}$.

Por outro lado, suponhamos que a é um quadrado módulo $4p$. Para cada inteiro positivo n, mostraremos que existe $b_n \in \mathbb{Z}_p$, tal que $a \equiv b_n^2 \pmod{4p^n}$. Faremos por indução. Para $n = 1$, segue diretamente da hipótese, pois existe $b_1 \in \mathbb{Z}_p$, tal que $a \equiv b_1^2 \pmod{4p}$. Suponhamos que $a \equiv b_k^2 \pmod{4p^k}$. Então existe $y \in \mathbb{Z}_p$, tal que $a = 4p^k y + b_k^2$.

Observamos que, se p divide b_k, então p divide $4p^k y + b_k^2 = a$, o que contradiz o fato de a ser primo com p, logo, p não divide b_k. Pelo Lema 2.25, segue que b_k é uma unidade em $\mathbb{Z}_p$. Dessa forma, podemos definir $d_k = b_k^{-1} c_k$, em que $c_k = p^k y \equiv 0 \pmod{p^k}$. Então $d_k \equiv 0 \pmod{p^k}$ e

$$a = b_k^2 + 4c_k = b_k^2 + 4d_k b_k = b_k^2 + 4d_k b_k + 4d_k^2 - 4d_k^2 = (b_k + 2d_k)^2 - 4d_k^2.$$

Note que $d_k \equiv 0 \pmod{p^k}$ implica que $4d_k^2 \equiv 0 \pmod{4p^{2k}}$. Posto $b_{k+1} = b_k + 2d_k$, segue que

$$\begin{aligned} a = (b_k + 2d_k)^2 - 4d_k^2 = b_{k+1}^2 - 4d_k^2 &\implies a \equiv b_{k+1}^2 \pmod{4p^{2k}} \\ &\implies a \equiv b_{k+1}^2 \pmod{4p^{k+1}}. \end{aligned}$$

Isso conclui a indução e, em particular, $a \equiv b_n^2 \pmod{4p^n}$ para todo inteiro positivo n. Agora, pelo Lema 2.27, basta mostrar que a sequência $(b_n)_n$ é de Cauchy. Isso ocorre pois $d_n \equiv 0 \pmod{p^n}$, assim, p^n divide $2d_n = b_{n+1} - b_n$. Isso implica que $|b_n - b_{n+1}|_p \leq p^{-n}$ e, portanto, a sequência $(b_n)_n$ é de Cauchy. □

Utilizando diretamente o Teorema 3.7 e o Lema 3.8 podemos concluir o seguinte.

Corolário 3.9. *Seja $f(x)$ um polinômio mônico de grau n com coeficientes em $\mathbb{Z}_p$. Assuma que $\bar{f}(x)$ não tem raízes múltiplas. Seja r o número de fatores irredutíveis de $\bar{f}(x)$ sobre $\mathbb{F}_p$. Então $r \equiv n \pmod 2$ se, e somente se, $D(f)$ é um quadrado módulo $4p$.*

Com mais esse corolário em mãos, podemos ainda provar o próximo resultado, que será importante adiante.

Corolário 3.10. *Seja $g(x)$ um polinômio de grau n sobre $\mathbb{F}_2$ sem raízes múltiplas, e r o número de fatores irredutíveis de $g(x)$ sobre $\mathbb{F}_2$. Seja $f(x)$ um polinômio mônico sobre $\mathbb{Z}_2$, tal que $\bar{f}(x) = g(x)$. Então $r \equiv n \pmod 2$ se, e somente se, $D(f) \equiv 1 \pmod 8$.*

Demonstração. Mostraremos inicialmente que os únicos quadrados módulo 8 em $\mathbb{Z}_2$ são 0, 1 e 4. Seja $b = b_0 + 2b_1 + 4b_2 + \cdots$, com $b_0, b_1, \cdots \in \{0, 1\}$ a expansão 2-ádica de b. Se $a = b^2$, então

$$a \equiv b^2 \equiv b_0^2 + 4b_1^2 + 4b_0b_1 \pmod 8.$$

Analisando todas as possibilidades para b_0 e b_1, obtemos $a \equiv 0, 1, 4 \pmod 8$, como gostaríamos.

Pelo Corolário 3.9, segue que

$$\begin{aligned} r \equiv n \pmod 2 &\iff D(f) \text{ é um quadrado módulo } 8 \\ &\iff D(f) \equiv 0, 1, 4 \pmod 8. \end{aligned}$$

Pela Observação 3.3, $D(f)$ é primo com 2, ou seja, é ímpar. Portanto,

$$r \equiv n \pmod 2 \iff D(f) \equiv 1 \pmod 8.$$

□

3.2 A Resultante

O objetivo agora é apresentar um método mais simples para calcular o discriminante de qualquer trinômio. Para isso, é necessário introduzir o conceito de resultante de dois polinômios.

Definição 3.11. *Sejam $f(x), g(x) \in F[x]$. Consideramos $\beta_1, \ldots, \beta_m$ as raízes de $g(x)$ em alguma extensão de F (contadas com multiplicidade), b o coeficiente líder de $g(x)$ e $n = \partial(f(x))$. A resultante de $f(x)$ e $g(x)$ é dada por*

$$R(f, g) = b^n \prod_{j=1}^{m} f(\beta_j).$$

Exemplo 3.12. *Sejam* $f(x) = 2x^2 - 3x + 1$ *e* $g(x) = 3x^2 + x - 2$ *polinômios em* $\mathbb{Q}[x]$. *As raízes de* $g(x)$ *são* $2/3$ *e* -1. *Assim,*

$$R(f,g) = 3^2(f(2/3) \cdot f(-1)) = 9 \cdot (-1/9) \cdot 6 = -6.$$

A seguir temos algumas propriedades básicas sobre $R(f,g)$.

Lema 3.13. *Sejam* $f(x), f_1(x), f_2(x), g(x), g_1(x), g_2(x) \in F[x], n = \partial(f(x)), n_1 = \partial(f_1(x)), n_2 = \partial(f_2(x)), m = \partial(g(x)), m_1 = \partial(g_1(x)), m_2 = \partial(g_2(x))$ *e* b *o coeficiente líder de* $g(x)$. *Então*

(i) $R(g,f) = (-1)^{mn}R(f,g)$;

(ii) Se $f(x) = g(x)q(x) + r(x)$, *então* $R(f,g) = b^{n-s}R(r,g)$, *em que* $s = \partial(r(x))$;

(iii) Se α *e* β *são constantes e pelo menos uma é não nula, então* $R(\alpha,\beta) = 1$;

(iv) $R(f_1f_2,g) = R(f_1,g)R(f_2,g)$;

(v) $R(f,g_1g_2) = R(f,g_1)R(f,g_2)$;

(vi) Se α *é constante, então* $R(f,\alpha) = \alpha^n = R(\alpha,f)$;

(vii) $R(f,x^t) = R(f,x)^t = f(0)^t$.

Demonstração. Consideramos $f(x) = a\prod_{i=1}^{n}(x-\alpha_i)$ e $g(x) = b\prod_{j=1}^{m}(x-\beta_j)$.

(i) Temos

$$R(f,g) = b^n\prod_{j=1}^{m}f(\beta_j) = b^n\prod_{j=1}^{m}(a\prod_{i=1}^{n}(\beta_j-\alpha_i)) = a^mb^n\prod_{j=1}^{m}\prod_{i=1}^{n}(\beta_j-\alpha_i).$$

Além disso,

$$R(g,f) = a^m\prod_{i=1}^{n}g(\alpha_i) = a^m\prod_{i=1}^{n}(b\prod_{j=1}^{m}(\alpha_i-\beta_j)) = a^mb^n\prod_{j=1}^{m}\prod_{i=1}^{n}(\alpha_i-\beta_j).$$

Logo,

$$\begin{aligned} R(g,f) = a^mb^n\prod_{j=1}^{m}\prod_{i=1}^{n}(\alpha_i-\beta_j) &= (-1)^{mn}a^mb^n\prod_{j=1}^{m}\prod_{i=1}^{n}(\beta_j-\alpha_i) \\ &= (-1)^{mn}R(f,g). \end{aligned}$$

(ii) Temos $R(r,g) = b^s\prod_{j=i}^{m}r(\beta_j)$, assim $\prod_{j=1}^{m}r(\beta_j) = b^{-s}R(r,g)$. Além disso,

$$R(f,g) = b^n\prod_{j=1}^{m}f(\beta_j) = b^n\prod_{j=1}^{m}(g(\beta_j)q(\beta_j)+r(\beta_j)) = b^n\prod_{j=1}^{m}r(\beta_j).$$

Daí,

$$R(f,g) = b^n \prod_{j=1}^{m} r(\beta_j) = b^{n-s} R(r,g).$$

(iii) É imediato da definição. Note que pedimos uma constante não nula para evitar a indeterminação 0^0.

(iv) Temos

$$\begin{aligned} R(f_1 f_2, g) = b^{n_1+n_2} \prod_{j=1}^{m} f_1(\beta_j) f_2(\beta_j) &= b^{n_1} \prod_{j=1}^{m} f_1(\beta_j) b^{n_2} \prod_{j=1}^{m} f_2(\beta_j) \\ &= R(f_1,g) R(f_2,g). \end{aligned}$$

(v) Pelos itens (i) e (iv), segue que

$$R(f, g_1 g_2) = (-1)^{(g_1+g_2)n} R(g_1 g_2, f) = (-1)^{g_1 n} R(g_1, f)(-1)^{g_2 n} R(g_2, f) = R(f,g_1) R(f,g_2).$$

(vi) É imediato da definição.

(vii) Temos

$$R(f, x^t) = \prod_{j=1}^{t} f(0) = f(0)^t = R(f,x)^t.$$

□

Observação 3.14. *Veja que $R(f,g)$ é um polinômio simétrico nas raízes de $g(x)$, isso implica que $R(f,g) \in F$. Também, se $f(x)$ é um polinômio mônico, então, pelo Lema 3.6 e a definição anterior, vale que*

$$D(f) = (-1)^{n(n-1)/2} R(f', f).$$

A fim de calcular o discriminante de um trinômio qualquer, é necessário, primeiro, calcular a resultante entre dois binômios.

Lema 3.15. *Seja $d = \mathrm{mdc}(r,s), r = dr_1$ e $s = ds_1$. Então*

$$R(x^r - \alpha, x^s - \beta) = (-1)^s (\alpha^{s_1} - \beta^{r_1})^d,$$

em que α, β são elementos do corpo F.

Demonstração. Façamos primeiro o caso em que $\beta = 0$. Pelo Lema 3.13 (vii), temos

$$R(x^r - \alpha, x^s - \beta) = R(x^r - \alpha, x^s) = (0^r - \alpha)^s = (-\alpha)^{s_1 d} = (-1)^s [\alpha^{s_1} - \beta^{r_1}]^d.$$

Suponhamos agora que $\beta \neq 0$. Mostraremos inicialmente que se o resultado vale para o par (r, s), então também vale para o par (s, r). Se vale para o par (r, s), então $R(x^r - \alpha, x^s - \beta) = (-1)^s(\alpha^{s_1} - \beta^{r_1})^d$. Vejamos que vale para o par (s, r), isto é, $R(x^s - \beta, x^r - \alpha) = (-1)^r(\beta^{r_1} - \alpha^{s_1})^d$. Pelo Lema 3.13, temos

$$\begin{aligned} R(x^s - \beta, x^r - \alpha) &= (-1)^{rs} R(x^r - \alpha, x^s - \beta) \\ &= (-1)^{rs}(-1)^s(\alpha^{s_1} - \beta^{r_1})^d \\ &= (-1)^{rs+s}[(-1)(\beta^{r_1} - \alpha^{s_1})]^d \\ &= (-1)^{rs+s+d}(\beta^{r_1} - \alpha^{s_1})^d. \end{aligned}$$

Vejamos que $rs + s + d \equiv r \pmod 2$. Observe que $rs + s + d = dr_1ds_1 + ds_1 + d = d(dr_1s_1 + s_1 + 1)$. Se d é par, então $rs + s + d$ e r também o são e vale $rs + s + d \equiv r \pmod 2$. Se d é ímpar, então $rs + s + d \equiv r_1s_1 + s_1 + 1 \pmod 2$. Se r_1 é ímpar, então r é ímpar e s_1 é par, pois $\text{mdc}(r_1, s_1) = 1$. Nesse caso, $r_1s_1 + s_1 + 1$ é ímpar e $rs + s + d \equiv r_1s_1 + s_1 + 1 \equiv r \pmod 2$. Se r_1 é par, então r é par, s_1 é ímpar e, consequentemente, $r_1s_1 + s_1 + 1$ é par e $rs + s + d \equiv r_1s_1 + s_1 + d \equiv r \pmod 2$. Em todos os casos, temos o desejado. Assim,

$$R(x^s - \beta, x^r - \alpha) = (-1)^{rs+s+d}(\beta^{r_1} - \alpha^{s_1})^d = (-1)^r(\beta^{r_1} - \alpha^{s_1})^d,$$

e a afirmação está provada.

Para provar o resultado faremos indução sobre $r + s$. Pela afirmação anterior, podemos supor, sem perda de generalidade, que $r \geq s$. Note que, para $s = 0$, vale

$$R(x^r - \alpha, x^s - \beta) = R(x^r - \alpha, 1 - \beta) = (1 - \beta)^r = (-1)^s(\alpha^{s_1} - \beta_1^r)^d.$$

Ou seja, o resultado vale para $r + s$ com $s = 0$ e, em particular, colocando $r = 1$, vale para $r + s = 1$. Suponhamos agora que vale para $r' + s' < r + s$ e vejamos que vale para $r + s$ com $s > 0$. Dividindo $x^r - \alpha$ por $x^s - \beta$, obtemos

$$x^r - \alpha = (x^s - \beta)x^{r-s} + x^{r-s}\beta - \alpha.$$

Utilizando (ii), (iv) e (vi) do Lema 3.13, obtemos

$$\begin{aligned} R(x^r - \alpha, x^s - \beta) &= R(x^{r-s}\beta - \alpha, x^s - \beta) \\ &= R(\beta(x^{r-s} - \alpha\beta^{-1}), x^s - \beta) \\ &= R(\beta, x^s - \beta)R(x^{r-s} - \alpha\beta^{-1}, x^s - \beta) \\ &= \beta^s R(x^{r-s} - \alpha\beta^{-1}, x^s - \beta). \end{aligned}$$

Agora, $(r-s)+s < r+s$. Assim, pela hipótese de indução, segue que

$$\begin{aligned} R(x^{r-s}-\alpha, x^s-\beta) &= \beta^s R(x^{r-s}-\alpha\beta^{-1}, x^s-\beta) \\ &= \beta^s(-1)^s[(\alpha\beta^{-1})^{s_1}-\beta^{r_1-s_1}]^d, \end{aligned}$$

em que $d = \text{mdc}(r-s, s)$ e $r-s = (r_1 d - s_1 d) = (r_1 - s_1)d$.

Note que

$$\begin{aligned} [(\alpha\beta^{-1})^{s_1}-\beta^{r_1-s_1}]^d &= [\alpha^{s_1}\beta^{-s_1}-\beta^{r_1}\beta^{-s_1}]^d \\ &= [(\alpha^{s_1}-\beta^{r_1})\beta^{-s_1}]^d \\ &= (\alpha^{s_1}-\beta^{r_1})^d\beta^{-s}. \end{aligned}$$

Logo,

$$\begin{aligned} R(x^r-\alpha, x^s-\beta) &= \beta^s(-1)^s[(\alpha\beta^{-1})^{s_1}-\beta^{r_1-s_1}]^d \\ &= \beta^s(-1)^s(\alpha^{s_1}-\beta^{r_1})^d\beta^{-s} \\ &= (-1)^s(\alpha^{s_1}-\beta^{r_1})^d. \end{aligned}$$

□

3.3 A Paridade do Número de Fatores Irredutíveis de $x^n + x^k + 1$

Iniciamos a seção com um teorema que nos fornece uma forma de calcular o discriminante de um trinômio sem precisar conhecer suas raízes.

Teorema 3.16. *Sejam n e k inteiros tais que $n > k > 0$. Consideramos $d = \text{mdc}(n,k)$, $n = n_1 d$ e $k = k_1 d$. Então, sobre um corpo de característica 0, temos*

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1}[n^{n_1} b^{n_1-k_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1}k^{k_1}a^{n_1}]^d.$$

Demonstração. Na Observação 3.14 vimos que $D(f) = (-1)^{n(n-1)/2}R(f', f)$. Assim, pelo Lema 3.13, segue que

$$\begin{aligned} D(x^n+ax^k+b) &= (-1)^{n(n-1)/2}R(nx^{n-1}+kax^{k-1}, x^n+ax^k+b) \\ &\overset{(i)}{=} (-1)^{n(n-1)/2}(-1)^{(n-1)n}R(x^n+ax^k+b, nx^{n-1}+kax^{k-1}) \\ &= (-1)^{3n(n-1)/2}R(x^n+ax^k+b, x^{k-1}(nx^{n-k}+ka)) \\ &\overset{(v)}{=} (-1)^{3n(n-1)/2}R(x^n+ax^k+b, x^{k-1})R(x^n+ax^k+b, nx^{n-k}+ka) \\ &\overset{(vii)}{=} (-1)^{3n(n-1)/2}(0^n+a0^k+b)^{k-1}R(x^n+ax^k+b, n(x^{n-k}+kan^{-1})) \\ &\overset{(v)}{=} (-1)^{3n(n-1)/2}b^{k-1}R(x^n+ax^k+b, n)R(x^n+ax^k+b, x^{n-k}+kan^{-1}) \\ &\overset{(vi)}{=} (-1)^{3n(n-1)/2}b^{k-1}n^nR(x^n+ax^k+b, x^{n-k}+kan^{-1}). \end{aligned}$$

Observe agora que $3n(n-1)/2$ e $n(n-1)/2$ têm a mesma paridade para qualquer valor de n. Dessa forma,

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} n^n R(x^n + ax^k + b, x^{n-k} + kan^{-1}). \tag{3.4}$$

Dividindo $x^n + ax^k + b$ por $x^{n-k} + kan^{-1}$, obtemos

$$x^n + ax^k + b = (x^{n-k} + kan^{-1})x^k + (a - kan^{-1})x^k + b.$$

Pelo Lema 3.13.(ii), segue que

$$R(x^n + ax^k + b, x^{n-k} + kan^{-1}) = R((a - kan^{-1})x^k + b, x^{n-k} + kan^{-1}).$$

Fazendo $\alpha = (a - kan^{-1}) \neq 0$ e $\beta = kan^{-1}$, e utilizando o Lema 3.13 novamente, vem que

$$\begin{aligned} R(x^n + ax^k + b, x^{n-k} + kan^{-1}) &= R(\alpha x^k + b, x^{n-k} + \beta) \\ &= R(\alpha(x^k + b\alpha^{-1}), x^{n-k} + \beta) \\ &= R(\alpha, x^{n-k} + \beta) R(x^k + b\alpha^{-1}, x^{n-k} + \beta) \\ &= \alpha^{n-k} R(x^k - (-b\alpha^{-1}), x^{n-k} - (-\beta)) \\ &= \alpha^{n-k} (-1)^{n-k} [(-b\alpha^{-1})^{n_1-k_1} - (-\beta^{k_1})]^d, \end{aligned}$$

em que a última igualdade vale pelo Lema 3.15. Voltando com os valores de α e β nos colchetes e fazendo mais algumas manipulações, obtemos

$$\begin{aligned} R(x^n + ax^k + b, x^{n-k} + kan^{-1}) &= \alpha^{n-k}(-1)^{n-k}[(-b\alpha^{-1})^{n_1-k_1} - (-\beta^{k_1})]^d \\ &= \alpha^{n-k}(-1)^{n-k}\left[(-b(a - akn^{-1})^{-1})^{n_1-k_1} - (-kan^{-1})^{k_1}\right]^d \\ &= \alpha^{n-k}(-1)^{n-k}\left[(-b(an^{-1}(n-k))^{-1})^{n_1-k_1} - (-kan^{-1})^{k_1}\right]^d \\ &= \alpha^{n-k}(-1)^{n-k}[(-1)^{n_1-k_1} b^{n_1-k_1} n^{n_1-k_1} a^{-(n_1-k_1)} (n-k)^{-(n_1-k_1)} - \\ &\quad - (-1)^{k_1} k^{k_1} a^{k_1} n^{-k_1}]^d. \end{aligned}$$

Colocando $n^{-k_1} a^{-(n_1-k_1)} (n-k)^{-(n_1-k_1)}$ em evidência dentro dos colchetes, segue que

$$\begin{aligned} R(x^n + ax^k + b, x^{n-k} + kan^{-1}) &= \alpha^{n-k}(-1)^{n-k}[(n^{-k_1} a^{-(n_1-k_1)} (n-k)^{-(n_1-k_1)})[(-1)^{n_1-k_1} b^{n_1-k_1} \\ &\quad n^{n_1} - (-1)^{k_1} k^{k_1} a^{n_1} (n-k)^{n_1-k_1}]]^d \\ &= \alpha^{n-k}(-1)^{n-k}[n^{-k_1} a^{-(n_1-k_1)} (n-k)^{-(n_1-k_1)}]^d [(-1)^{n_1-k_1} b^{n_1-k_1} \\ &\quad n^{n_1} - (-1)^{k_1} k^{k_1} a^{n_1} (n-k)^{n_1-k_1}]^d \\ &= \alpha^{n-k}(-1)^{n-k}[n^{-k} a^{-(n-k)} (n-k)^{-(n-k)}][(-1)^{n_1-k_1} b^{n_1-k_1} \\ &\quad n^{n_1} - (-1)^{k_1} k^{k_1} a^{n_1} (n-k)^{n_1-k_1}]^d. \end{aligned}$$

Disto e da Equação (3.4), segue que

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} n^n \alpha^{n-k} (-1)^{n-k} [n^{-k} a^{-(n-k)} (n-k)^{-(n-k)}] \\ [(-1)^{n_1-k_1} b^{n_1-k_1} n^{n_1} - (-1)^{k_1} k^{k_1} a^{n_1} (n-k)^{n_1-k_1}]^d.$$

Mas,

$$\begin{aligned} n^n \alpha^{n-k} n^{-k} a^{-(n-k)} (n-k)^{-(n-k)} &= n^{n-k} (a - kan^{-1})^{n-k} a^{-(n-k)} (n-k)^{-(n-k)} \\ &= n^{n-k} (a(n-k)n^{-1})^{n-k} a^{-(n-k)} (n-k)^{-(n-k)} \\ &= n^{n-k} a^{n-k} (n-k)^{n-k} n^{-(n-k)} a^{-(n-k)} (n-k)^{-(n-k)} \\ &= 1. \end{aligned}$$

Assim,

$$\begin{aligned} D(x^n + ax^k + b) &= (-1)^{n(n-1)/2} b^{k-1} n^n \alpha^{n-k} (-1)^{n-k} [n^{-k} a^{-(n-k)} (n-k)^{-(n-k)}] \\ &\quad [(-1)^{n_1-k_1} b^{n_1-k_1} n^{n_1} - (-1)^{k_1} k^{k_1} a^{n_1} (n-k)^{n_1-k_1}]^d \\ &= (-1)^{n(n-1)/2} b^{k-1} (-1)^{n-k} [(-1)^{n_1-k_1} b^{n_1-k_1} n^{n_1} - (-1)^{k_1} k^{k_1} a^{n_1} (n-k)^{n_1-k_1}]^d \\ &= (-1)^{n(n-1)/2} b^{k-1} [(-1)^{n_1-k_1} (-1)^{n_1-k_1} b^{n_1-k_1} n^{n_1} - (-1)^{k_1} k^{k_1} a^{n_1} (n-k)^{n_1-k_1}]^d \\ &= (-1)^{n(n-1)/2} b^{k-1} [b^{n_1-k_1} n^{n_1} + (-1)^{n_1+1} k^{k_1} a^{n_1} (n-k)^{n_1-k_1}]^d. \end{aligned}$$

Portanto,

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} [n^{n_1} b^{n_1-k_1} + (-1)^{n_1+1} (n-k)^{n_1-k_1} k^{k_1} a^{n_1}]^d.$$

□

Como aplicação do teorema anterior, vamos determinar a paridade do número de fatores irredutíveis do trinômio $x^n + x^k + 1$ sobre $\mathbb{F}_2$.

Corolário 3.17. *Sejam n e k inteiros tais que $n > k > 0$. Assuma que n e k tenham paridades diferentes. Então $x^n + x^k + 1$ tem um número par de fatores irredutíveis (e portanto é redutível) sobre $\mathbb{F}_2$ nos seguintes casos:*

(i) n é par, k é ímpar, $n \neq 2k$ e $nk/2 \equiv 0, 1 \pmod 4$;

(ii) n é ímpar, k é par, $k \nmid 2n$ e $n \equiv 3, 5 \pmod 8$;

(iii) n é ímpar, k é par, $k \mid 2n$ e $n \equiv 1, 7 \pmod 8$.

Em todos os outros casos, $x^n + x^k + 1$ tem um número ímpar de fatores irredutíveis sobre $\mathbb{F}_2$.

Demonstração. Mostraremos inicialmente que $x^n + x^k + 1$ e sua derivada, $nx^{n-1} + kx^{k-1}$, não têm raízes em comum em nenhum dos casos. Sobre $\mathbb{F}_2$, a derivada no item (i) fica x^{k-1}.

Também, $\alpha^{k-1} = 0$ se, e somente se, $\alpha = 0$. Ou seja, a única raiz da derivada é 0, que não é raiz de $x^n + x^k + 1$. Nos itens (ii) e (iii), a derivada fica x^{n-1} e um raciocínio análogo mostra, novamente, que o polinômio e sua derivada não têm raízes em comum. Com essa informação, o Teorema 1.33 garante que $x^n + x^k + 1$ não tem raízes múltiplas. Feito isso, podemos utilizar o Corolário 3.9.

Consideramos $f(x) = x^n + x^k + 1 \in \mathbb{Z}_2[x]$. Pelo Teorema 3.16, temos

$$D(x^n + x^k + 1) = (-1)^{n(n-1)/2}[n^{n_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1}k^{k_1}]^d. \tag{3.5}$$

Além disso, lembramos que, para qualquer inteiro q, vale $\alpha^{2q} \equiv 1 \pmod 8$ e $\alpha^{2q+1} \equiv \alpha \pmod 8$, fato que será importante no que segue. Consideramos $d = \text{mdc}(n,k)$, $n = n_1 d$ e $k = k_1 d$. Vamos analisar cada um dos casos.

(i) Observamos que d e k_1 são ímpares e n_1 é par. Veja que, se $n_1 = 2$, então

$$n > k > 0 \implies 2d > k_1 d \implies 2 > k_1 \implies k_1 = 1 \implies k = d \implies n = 2k.$$

Mas, por hipótese, $n \neq 2k$, logo, $n_1 \geq 4$ e, consequentemente, $n^{n_1} \equiv 0 \pmod 8$. Daí,

$$\begin{aligned}(-1)^{n(n-1)/2}[n^{n_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1}k^{k_1}]^d &\equiv (-1)^{n(n-1)/2}[-(n-k)k]^d \\ &\equiv (-1)^{n(n-1)/2}[-nk+k^2]^d \\ &\equiv (-1)^{n(n-1)/2}[-nk+1] \pmod 8.\end{aligned}$$

Com isso e a Equação (3.5), temos

$$\begin{aligned}D(x^n + x^k + 1) &\equiv (-1)^{n(n-1)/2}[n^{n_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1}k^{k_1}]^d \\ &\equiv (-1)^{n(n-1)/2}[-nk+1] \pmod 8.\end{aligned}$$

Se $nk/2 \equiv 0 \pmod 4$, então $nk \equiv 0 \pmod 8$ e, como k é ímpar, segue que $n \equiv 0 \pmod 8$. Logo,

$$D(x^n + x^k + 1) \equiv (-1)^{n(n-1)/2}[-nk+1] \equiv 1 \pmod 8.$$

Se $nk/2 \equiv 1 \pmod 4$, então $nk \equiv 2 \pmod 8$ e $nk \not\equiv 0 \pmod 4$. Assim, $n \equiv 2 \pmod 4$ e

$$D(x^n + x^k + 1) \equiv (-1)^{n(n-1)/2}[-2+1] \equiv (-1)[-1] \equiv 1 \pmod 8.$$

Em ambos os casos, $D(x^n + x^k + 1) \equiv 1 \pmod 8$. Pelo Corolário 3.10, o número de fatores irredutíveis de $x^n + x^k + 1$ tem a mesma paridade de n, que, nesse caso, é par. Isso finaliza o primeiro caso.

(ii) Observamos que d e n_1 são ímpares e k_1 é par. Veja que, se $k_1 = 2$, então $k = 2d$ e

$$2n = 2n_1 d = kn_1 \implies k \mid 2n.$$

Mas, por hipótese, $k \nmid 2n$, logo, $k_1 \geq 4$ e, consequentemente, $k^{k_1} \equiv 0 \pmod 8$. Daí,

$$(-1)^{n(n-1)/2}[n^{n_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1}k^{k_1}]^d \equiv (-1)^{n(n-1)/2}[n]^d \equiv \pm n \pmod 8.$$

Com isso e a Equação (3.5), temos

$$D(x^n + x^k + 1) \equiv \pm n \equiv 3, 5 \pmod 8.$$

Ou seja, $D(x^n+x^k+1) \not\equiv 1 \pmod 8$. Pelo Corolário 3.10, o número de fatores irredutíveis de x^n+x^k+1 tem paridade diferente de n, que, nesse caso, é ímpar. Isso finaliza o segundo caso.

(iii) Observamos que d e n_1 são ímpares e k_1 é par. Podemos escrever $k = 2t, t \in \mathbb{Z}$. Assim,

$$k \mid 2n \implies 2t \mid 2n \implies t \mid n.$$

Com isso, $d = \text{mdc}(k, n) = \text{mdc}(2t, n) = \text{mdc}(t, n) = t$. Logo, $2t = k = k_1 d = k_1 t$ e, consequentemente, $k_1 = 2$ e $k^{k_1} \equiv k^2 \equiv (2d)^2 \equiv 4 \pmod 8$, pois d é ímpar. Daí,

$$\begin{aligned}(-1)^{n(n-1)/2}[n^{n_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1}k^{k_1}]^d &\equiv (-1)^{n(n-1)/2}[n + (n-k)4]^d \\ &\equiv (-1)^{n(n-1)/2}[5n - 4k]^d \\ &\equiv \pm 5n \pmod 8.\end{aligned}$$

Com isso e a Equação (3.5), temos

$$D(x^n + x^k + 1) \equiv \pm 5n \equiv 3, 5 \pmod 8.$$

Novamente, $D(x^n + x^k + 1) \not\equiv 1 \pmod 8$ e, como no caso anterior, segue o resultado.

Resta mostrar que em todos os outros casos o polinômio $x^n + x^k + 1$ possui um número ímpar de fatores. Para isso, utilizaremos que, se $n = 2t, t \in \mathbb{Z}$, então $n(n-1)/2$ e t têm a mesma paridade, e que se $n = 2m + 1, m \in \mathbb{Z}$, então $n(n-1)/2$ e m têm a mesma paridade. Assim, $(-1)^{n(n-1)/2} = (-1)^t$ e $(-1)^{n(n-1)/2} = (-1)^m$, respectivamente. Vamos analisar os casos individualmente.

(i) Podemos escrever $n = 2t, t \in \mathbb{Z}$. Já vimos que $D(x^n + x^k + 1) \equiv (-1)^{n(n-1)/2}[-nk + 1] \pmod 8$. Vejamos o que ocorre se $n \neq 2k$ e $nk/2 \equiv 2, 3 \pmod 4$.

- $nk/2 \equiv 2 \pmod 4 \implies nk \equiv 4 \pmod 8$. Logo, $D(x^n + x^k + 1) \equiv (-1)^t[-4 + 1] \equiv 3, 5 \pmod 8$.
- $nk/2 \equiv 3 \pmod 4 \implies nk \equiv 6 \pmod 8$. Logo, $D(x^n + x^k + 1) \equiv (-1)^t[-6 + 1] \equiv 3, 5 \pmod 8$.

Em ambos os casos, $D(x^n + x^k + 1) \not\equiv 1 \pmod 8$ e, pelo Corolário 3.10, a quantidade de fatores irredutíveis e n têm paridades diferentes. Portanto, $x^n + x^k + 1$ tem um número ímpar de fatores irredutíveis. Para o caso em que $n = 2k$, temos $d = k, n_1 = 2$ e $k_1 = 1$. Assim,

$$\begin{aligned} D(x^n + x^k + 1) &\equiv (-1)^{n(n-1)/2}[n^{n_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1}k^{k_1}]^d \\ &\equiv -[(2k)^2 - (2k-k)k]^d \\ &\equiv -[3k^2] \\ &\equiv -3 \pmod 8. \end{aligned}$$

Novamente, $D(x^n + x^k + 1) \not\equiv 1 \pmod 8$ e segue o resultado.

(ii) Como n é ímpar, digamos $n = 2m + 1, m \in \mathbb{Z}$, não faz sentido falar sobre $n \equiv 0, 2 \pmod 8$. Já vimos que $D(x^n + x^k + 1) \equiv (-1)^{n(n-1)/2}n \pmod 8$. Vejamos o que ocorre se $n \equiv 1, 7 \pmod 8$.

- $n \equiv 1 \pmod 8 \implies n = 2m + 1 = 8q_1 + 1, q_1 \in \mathbb{Z} \implies m = 4q_1$ é par. Logo, $D(x^n + x^k + 1) \equiv 1 \pmod 8$.
- $n \equiv 7 \pmod 8 \implies n = 2m + 1 = 8q_2 + 7, q_2 \in \mathbb{Z} \implies m = 4q_2 + 3$ é ímpar. Logo, $D(x^n + x^k + 1) \equiv -7 \equiv 1 \pmod 8$.

Em ambos os casos, $D(x^n + x^k + 1) \equiv 1 \pmod 8$ e, pelo Corolário 3.10, segue que o que gostaríamos.

(iii) Consideramos novamente $n = 2m + 1$ e, nesse caso, já vimos que $D(x^n + x^k + 1) \equiv (-1)^{n(n-1)/2}5n \pmod 8$. Vejamos o que ocorre se $n \equiv 3, 5 \pmod 8$.

- $n \equiv 3 \pmod 8 \implies n = 2m + 1 = 8q_3 + 3, q_3 \in \mathbb{Z} \implies m = 4q_3 + 1$ é ímpar. Logo, $D(x^n + x^k + 1) \equiv -15 \equiv 1 \pmod 8$.
- $n \equiv 5 \pmod 8 \implies n = 2m + 1 = 8q_4 + 5, q_4 \in \mathbb{Z} \implies m = 4q_4 + 2$ é par. Logo, $D(x^n + x^k + 1) \equiv 25 \equiv 1 \pmod 8$.

Novamente, $D(x^n + x^k + 1) \equiv 1 \pmod 8$ em ambos os casos e, pelo Corolário 3.10, segue o resultado.

□

Vamos ver o que acontece quando n e k têm a mesma paridade. Para o caso em que ambos são ímpares, utilizaremos o conceito de polinômio recíproco para fazer a análise.

Definição 3.18. *Seja* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$, *com* $a_n \neq 0$. *O polinômio recíproco de* $f(x)$ *é dado por*

$$f^*(x) = x^n f(1/x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n.$$

Lema 3.19. *Seja* $f(x) \in \mathbb{F}_q[x]$ *um polinômio de grau* n. *Então* $f^*(x)$ *tem o mesmo número de fatores irredutíveis de* $f(x)$.

Demonstração. Temos $(f^*)^*(x) = x^n f^*(1/x) = x^n((1/x)^n f(x)) = f(x)$. Isto é, $(f^*)^*(x) = f(x)$. Além disso, se $g(x) \in \mathbb{F}_q[x]$ tem grau m, então

$$(fg)^*(x) = x^{n+m}(fg)(1/x) = x^n f(1/x) x^m g(1/x) = f^*(x)g^*(x).$$

Consideramos $f(x) = f_1(x) \ldots f_r(x)$ a fatoração de $f(x)$. Então $f_1(x), \ldots, f_r(x)$ são todos irredutíveis e isso implica que os seus respectivos recíprocos também o são. Do contrário, existiriam $i \in \{1, 2, \ldots, r\}$ e $g(x), h(x) \in \mathbb{F}_q[x]$, tais que $f_i^*(x) = g(x)h(x)$, com $\partial(g(x)), \partial(h(x)) > 0$. Tomando os recíprocos de cada lado, temos $f_i(x) = g^*(x)h^*(x)$, com $\partial(g^*(x)), \partial(h^*(x)) > 0$, o que contradiz a irredutibilidade de $f_i(x)$. Portanto, temos a seguinte fatoração $f^*(x) = f_1^*(x) \ldots f_r^*(x)$ e o lema está provado. □

Agora, $x^n + x^{n-k} + 1 = x^n((1/x)^n + (1/x)^k + 1)$. Ou seja, $(x^n + x^k + 1)^* = x^n + x^{n-k} + 1$. Pelo lema anterior, fazer a análise da paridade dos fatores irredutíveis de $x^n + x^k + 1$ equivale a analisar a paridade de $x^n + x^{n-k} + 1$, e como n é ímpar e $n - k$ é par, basta utilizar o corolário anterior.

No caso em que ambos são pares, digamos $n = 2q_1$ e $k = 2q_2$ com $q_1, q_2 \in \mathbb{Z}$, pelo Teorema 1.4, temos $x^n + x^k + 1 = x^{2q_1} + x^{2q_2} + 1 = (x^{q_1} + x^{q_2} + 1)^2$. Assim, $x^n + x^k + 1$ e $x^{q_1} + x^{q_2} + 1$ têm a mesma quantidade de fatores irredutíveis. Portanto, basta fazer a análise nesse novo polinômio utilizando o que já vimos.

Capítulo 4

Classificação de Pares 3-sparse para $q = 2$ e $q = 4$

Neste capítulo investigamos para quais valores de n o par ordenado (n, q) é 3-sparse, isto é, para quais valores de n o polinômio $x^n - 1$ se fatora em binômios e trinômios sobre $\mathbb{F}_q$, em que q é uma potência de 2.

Iniciamos com a definição de 3-sparse, seguida de alguns exemplos, propriedades, e resultados preliminares sobre a fatoração de $x^n - 1$.

O Teorema 4.13 caracteriza completamente os pares $(n, 2)$ que são 3-sparse, para $n > 1$ ímpar, isso ocorre se, e somente se $n \in \{3^k, 7^k\}$, para algum $k \geq 1$. A demonstração envolve uma análise detalhada dos polinômios ciclotômicos $\Phi_{3^k}(x)$ e $\Phi_{7^k}(x)$ sobre $\mathbb{F}_2$.

Na sequência, o Teorema 4.17 classifica todos os pares $(n, 4)$ que são 3-sparse, para $n > 1$ ímpar, isso ocorre se, e somente se $n \in \{3^k, 5^k, 7^k, 3^m \cdot 5^k, 3 \cdot 7^k\}$, para certos $k, m \geq 1$. Novamente isso envolve uma análise detalhada sobre os respectivos polinômios ciclotômicos sobre $\mathbb{F}_2$.

4.1 Preparação

Definição 4.1. *Para qualquer inteiro positivo n, o par (n, q) é dito 3-sparse se os fatores irredutíveis do polinômio $x^n - 1$ sobre $\mathbb{F}_q$ são todos binômios e trinômios.*

Exemplo 4.2. *Como $x - 1$ é um binômio irredutível sobre $\mathbb{F}_q$, o par $(1, q)$ é 3-sparse.*

Exemplo 4.3. *Pelo Exemplo 1.29, a fatoração de $x^3 - 1$ sobre $\mathbb{F}_2$ é dada por*

$$x^3 - 1 = \prod_{d|3} \Phi_d(x) = (x - 1)(x^2 + x + 1).$$

Logo, o par $(3, 2)$ é 3-sparse. Já pelo Exemplo 1.30, segue que

$$x^5 - 1 = \prod_{d|5} \Phi_d(x) = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

é a fatoração de $x^5 - 1$ sobre $\mathbb{F}_2$. Sendo assim, o par $(5, 2)$ não é 3-sparse.

Exemplo 4.4. *Sejam n e s inteiros positivos. Então (n, q) é 3-sparse se, e somente se, $(2^s n, q)$ é 3-sparse. De fato, como q é uma potência de dois, o Teorema 1.4 implica que $x^{2^s n} - 1 = (x^n - 1)^{2^s}$. Consideramos a fatoração $x^n - 1 = f_1(x) \cdots f_r(x)$, então*

$$x^n - 1 = f_1(x) \cdots f_r(x) \implies x^{2^s n} - 1 = (x^n - 1)^{2^s} = (f_1(x) \cdots f_r(x))^{2^s}.$$

Ou seja, $x^n - 1$ e $x^{2^s n} - 1$ têm os mesmos fatores irredutíveis.

Esse exemplo nos mostra que é suficiente estudar os pares (n, q), em que $n > 1$ é ímpar.

Exemplo 4.5. *Seja (n, q) 3-sparse. Então (d, q) é 3-sparse para todo $d \geq 1$ divisor de n. De fato, como $d \mid n$, temos $x^d - 1 \mid x^n - 1$. Logo, todo fator irredutível de $x^d - 1$ é também um fator irredutível de $x^n - 1$. Como todos os fatores irredutíveis de $x^n - 1$ são binômios e trinômios, o mesmo vale para $x^d - 1$, concluindo a demonstração.*

Teorema 4.6. *Seja K uma extensão com grau par de $\mathbb{F}_2$. Então todo trinômio de grau par sobre K é redutível, exceto os trinômios da forma $x^{2d} + ax^d + b$ para os quais o polinômio quadrático $t^2 + at + b$ não possui raízes em K.*

Demonstração. [15, Corollary 5.1] □

O lema seguinte caracteriza os binômios divisores de $x^n - 1$ sobre $\mathbb{F}_q$.

Lema 4.7. *Sejam t e n inteiros positivos e $a \in \mathbb{F}_q^*$ um elemento de ordem M. Então $x^t - a$ divide $x^n - 1$ se, e somente se, tM divide n.*

Demonstração. Pelo algoritmo da divisão, podemos escrever $n = tq_2 + r, 0 \leq r < t$. Temos $x^t \equiv a \pmod{x^t - a}$. Com isso,

$$x^n - 1 \equiv (x^t)^{q_2} x^r - 1 \equiv a^{q_2} x^r - 1 \pmod{x^t - a}.$$

Então $x^t - a$ divide $x^n - 1$ se, e somente se, $x^t - a$ divide $a^{q_2} x^r - 1$. Mas o grau de $a^{q_2} x^r - 1$ é menor que o grau de $x^t - a$. Donde $x^t - a$ divide $a^{q_2} x^r - 1$ se, e somente se, $a^{q_2} x^r - 1 = 0$. O que ocorre se, e somente se, $a^{q_2} = 1$ e $r = 0$. Assim, se $x^t - a$ divide $x^n - 1$, então $a^{q_2} = 1$ e $r = 0$, o que implica que M divide $q_2 = n/t$, pois M é a ordem de a. Segue que tM divide n.

Para a recíproca, se tM divide n, então $n = tMq_3, q_3 \in \mathbb{Z}$. Seja β uma raiz de $x^t - a$, então $\beta^t = a$, logo, $\beta^{tM} = a^M = 1$. Assim, $\beta^n = (\beta^{tM})^{q_3} = 1$. Isso implica que toda raiz de $x^t - a$ é, também, raiz de $x^n - 1$. Dessa forma, $x^t - a$ divide $x^n - 1$.

□

O próximo lema caracteriza uma classe especial de polinômios irredutíveis sobre $\mathbb{F}_2$.

Lema 4.8. *Sejam $t \geq 3$ um inteiro ímpar e $f(x)$ um polinômio irredutível sobre $\mathbb{F}_2$ que se fatora em dois trinômios de grau t sobre $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$. Então existe um inteiro positivo $k < t$, tal que $f(x)$ tem uma das seguintes formas*

(i) $F_{k,t}(x) = x^{2t} + x^{t+k} + x^{2k} + x^k + 1 = (x^t + \alpha x^k + 1)(x^t + \alpha^2 x^k + 1)$;

(ii) $G_{k,t}(x) = x^{2t} + x^{t+k} + x^{2k} + x^t + 1 = (x^t + \alpha x^k + \alpha)(x^t + \alpha^2 x^k + \alpha^2)$;

(iii) $H_{k,t}(x) = x^{2t} + x^t + x^{2k} + x^k + 1 = (x^t + x^k + \alpha)(x^t + x^k + \alpha^2)$.

Demonstração. Pelo Teorema 1.37, podemos considerar $\sigma\colon \mathbb{F}_4 \to \mathbb{F}_4$ o $\mathbb{F}_2$-automorfismo com $\sigma(\beta) = \beta^2$, para todo $\beta \in \mathbb{F}_4$. Se $g(x) = x^t + ax^k + b \in F4[x]$ é um dos fatores irredutíveis de $f(x)$ sobre $\mathbb{F}_2$, então $g(x) \notin \mathbb{F}_2[x]$, pois $f(x)$ é irredutível sobre $\mathbb{F}_2$. Isso implica que $a^2 \neq a$ ou $b^2 \neq b$. Logo, $\sigma(g(x)) = x^t + a^2x^k + b^2 \neq x^t + ax^k + b = g(x)$.

Em particular, se $f(x) = g(x)h(x), h(x) \in \mathbb{F}_4[x]$ é a fatoração de $f(x)$ em $\mathbb{F}_4[x]$, então $f(x) = \sigma(f(x)) = \sigma(g(x))\sigma(h(x))$, em que a primeira igualdade vale pois $f(x) \in \mathbb{F}_2$. Como $g(x)$ é um dos fatores irredutíveis de $f(x)$ e $\sigma(g(x)) \neq g(x)$, segue que $g(x) = \sigma(h(x))$ e $f(x) = g(x)\sigma(g(x))$. Assim, para ver quais as possíveis formas de $f(x)$, basta descobrir quais as possíveis formas $g(x)$, isto é, descobrir os possíveis valores de a e b.

Se $g(1) = 0$, então $g(x) = (x-1)p(x), p(x) \in \mathbb{F}_4[x]$ com $\partial(p(x)) = t - 1 \geq 2$, contradizendo a irredutibilidade de $g(x)$. Então $g(1) \neq 0$, ou seja, $a + b \neq 1$. Agora vamos analisar as possibilidades para a e b.

(i) $b = 1$. Para satisfazer $g(x) \notin \mathbb{F}_2[x]$, devemos ter $a \in \{\alpha, \alpha^2\}$. Com isso, obtemos $a + b = a + 1 \neq 0$. Temos então dois possíveis polinômios para $g(x)$: $x^t + \alpha x^k + 1$ e $x^t + \alpha^2 x^k + 1$.

(ii) $b = \alpha$. Já temos $g(x) \notin \mathbb{F}_2[x]$. Para que $a+b = a+\alpha \neq 1$, é necessário que $a \neq \alpha+1 = \alpha^2$. Logo, devemos ter $a \in \{1, \alpha\}$ (a não pode ser 0 pois $g(x)$ é um trinômio). Então temos mais dois possíveis polinômios para $g(x)$: $x^t + x^k + \alpha$ e $x^t + \alpha x^k + \alpha$.

(iii) $b = \alpha^2$. Já temos $g(x) \notin \mathbb{F}_2[x]$. Para que $a + b = a + \alpha^2 \neq 1$, é necessário que $a \neq \alpha^2 + 1 = \alpha$. Logo, devemos ter $a \in \{1, \alpha^2\}$. Então temos mais dois possíveis polinômios para $g(x)$: $x^t + x^k + \alpha^2$ e $x^t + \alpha^2 x^k + \alpha^2$.

Essa análise nos mostra que $g(x)$ tem uma das seguintes formas

$$\{x^t + \beta x^k + 1, x^t + x^k + \beta, x^t + \beta x^k + \beta\}, \tag{4.1}$$

em que $\beta \in \{\alpha, \alpha^2\}$. Observamos que $(\alpha^2)^2 = (\alpha + 1)^2 = \alpha^2 + 1 = \alpha$. Agora basta observar que, ao escolher qualquer polinômio em (4.1), aplicar σ e fazer o produto $f(x) = g(x)\sigma(g(x))$, obtemos exatamente os polinômios $F_{k,t}(x), G_{k,t}(x)$ e $H_{k,t}(x)$. □

4.2 Resultados Principais

Lema 4.9. *Seja p um primo ímpar. Consideramos $t = \mathrm{ord}_p(q)$ e suponhamos que (p, q) é 3-sparse. Se $t > 1$, então os fatores irredutíveis de $\Phi_p(x)$ sobre $\mathbb{F}_q$ são todos trinômios. Em particular, se q é uma potência par de 2, então $t = 2$ ou t é ímpar.*

Demonstração. Sabemos que $x^p - 1 = (x-1)\Phi_p(x)$. Como (p, q) é 3-sparse, os fatores irredutíveis de $\Phi_p(x)$ sobre $\mathbb{F}_q$ são todos binômios e trinômios. Dessa forma, é suficiente provar que o único binômio irredutível que divide $x^p - 1$ é $x - 1$.

É fácil ver que os binômios irredutíveis sobre $\mathbb{F}_2$ são da forma $x^d - c$, com $c \in \mathbb{F}_q^*$. Notamos que,

$$t = 1 \iff q \equiv 1 \pmod{p} \iff p \mid q - 1. \tag{4.2}$$

Definimos $M = \mathrm{ord}_q(c)$. Pelo Lema 4.7, $x^d - c$ divide $x^p - 1$ se, e somente se dM divide p. Como p é primo, essa divisão acontece se, e somente se, $dM = 1$ ou $dM = p$. Como $M = \mathrm{ord}_q(c)$, e a ordem de $\mathbb{F}_q$ é $q - 1$, segue que M divide $q - 1$. Assim, se $M = p$, então p divide $q - 1$ e, por (4.2), vem que $t = 1$, uma contradição com a hipótese. Logo, $M = 1$ e, consequentemente, $c = 1$. Por fim, devemos ter $d = 1$, pois $x^p - 1$ não é irredutível. Isso mostra que o único binômio irredutível que divide $x^p - 1$ é $x - 1$ e conclui a primeira parte da demonstração.

Para a segunda parte, suponhamos que t é par e vamos provar que $t = 2$. Pelo Teorema 1.25 e o que acabamos de provar, segue que

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1 = \prod_{i=1}^{l} (x^t + a_i x^{k_i} + b_i), \tag{4.3}$$

em que $l = (p-1)/t$, $a_i, b_i \in \mathbb{F}_q^*$ e $0 < k_i < t$, para todo $i \in \{1, 2, \ldots, l\}$.

Comparando os dois lados de (4.3), concluímos que $k_i = 1$ para algum $i \in \{1, 2, \ldots, l\}$. Sendo assim, existe um trinômio irredutível $x^t + ax + b \in \mathbb{F}_q[x]$. Pelo Lema 4.6, um trinômio irredutível em $\mathbb{F}_q[x]$ é da forma $x^{2d} + ax^d + b$. No caso de $x^t + ax + b$, devemos ter $d = 1$ e $t = 2$, como gostaríamos. □

Lema 4.10. *Sejam d e a inteiros positivos com $\mathrm{mdc}(d, a) = 1$. Se $d = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ é a fatoração de d, então*

$$\mathrm{ord}_d(a) = \mathrm{mmc}(\mathrm{ord}_{p_1^{\alpha_1}}(a), \ldots, \mathrm{ord}_{p_r^{\alpha_r}}(a)).$$

Além disso, para cada primo p e todo inteiro $\alpha \geq 1$, existe um inteiro $0 \leq \beta \leq \alpha - 1$, tal que

$$\mathrm{ord}_{p^\alpha}(a) = \mathrm{ord}_p(a) p^\beta.$$

Em particular, se $a^{\mathrm{ord}_p(a)} \not\equiv 1 \pmod{p^2}$, então $\mathrm{ord}_{p^\alpha}(a) = \mathrm{ord}_p(a) p^{\alpha-1}$.

Demonstração. Posto $t = \mathrm{ord}_d(a)$ e $m = \mathrm{mmc}(\mathrm{ord}_{p_1^{\alpha_1}}(a), \ldots, \mathrm{ord}_{p_r^{\alpha_r}}(a))$, mostraremos inicial-

mente que $t = m$. Temos

$$\begin{aligned} a^t \equiv 1 \pmod{d} &\implies a^t \equiv 1 \pmod{p_j^{\alpha_j}}, \forall j \in \{1, 2, \ldots, r\} \\ &\implies \operatorname{ord}_{p_j^{\alpha_j}}(a) \mid t, \forall j \in \{1, 2, \ldots, r\} \\ &\implies m \mid t. \end{aligned}$$

Por outro lado, como os p_j são primos entre si e $\operatorname{ord}_{p_j^{\alpha_j}}(a) \mid m$, para todo $j \in \{1, 2, \ldots, r\}$, temos

$$a^m \equiv 1 \pmod{p_j^{\alpha_j}}, \forall j \in \{1, 2, \ldots, r\} \implies a^m \equiv 1 \pmod{d} \implies t \mid m.$$

Isso implica que $t = m$ como gostaríamos. Vejamos agora que $\operatorname{ord}_{p^\alpha}(a) = \operatorname{ord}_p(a)p^\beta$, em que $0 \leq \beta \leq \alpha - 1$. Notamos que se $t_\alpha = \operatorname{ord}_{p^\alpha}(a)$, então

$$a^{t_\alpha} \equiv 1 \pmod{p^\alpha} \implies a^{t_\alpha} = A_\alpha p^\alpha + 1, A_\alpha \in \mathbb{Z}.$$

Elevando ambos os lados à potência p, temos

$$\begin{aligned} a^{t_\alpha p} \equiv \sum_{i=0}^{p} \binom{p}{i} (A_\alpha p^\alpha)^i &\equiv 1 + p(A_\alpha p^\alpha) + \binom{p}{2} (A_\alpha p^\alpha)^2 + \cdots + (A_\alpha p^\alpha)^p \\ &\equiv 1 \pmod{p^{\alpha+1}} \end{aligned}$$

Logo, $\operatorname{ord}_{p^{\alpha+1}}(a) \mid t_\alpha p$. Além disso, $a^{\operatorname{ord}_{p^{\alpha+1}}(a)} \equiv 1 \pmod{p^\alpha}$, donde, $t_\alpha \mid \operatorname{ord}_{p^{\alpha+1}}(a)$. Dessa forma, $\operatorname{ord}_{p^{\alpha+1}}(a)$ é múltiplo de t_α e divide $t_\alpha p$, ou seja, $\operatorname{ord}_{p^{\alpha+1}}(a) \in \{t_\alpha, t_\alpha p\}$. Utilizando esse fato, faremos indução sobre α. Para $\alpha = 1$, basta tomar $\beta = 0$. Suponhamos que o resultado vale para $\alpha > 1$, isto é, existe $0 \leq \beta \leq \alpha - 1$, tal que $t_\alpha = \operatorname{ord}_{p^\alpha}(a)p^\beta$. Pelo que fizemos anteriormente, $\operatorname{ord}_{p^{\alpha+1}}(a)$ é igual a $\operatorname{ord}_{p^\alpha}(a) = \operatorname{ord}_p(a)p^\beta$ ou $\operatorname{ord}_{p^\alpha}(a)p = \operatorname{ord}_p(a)p^{\beta+1}$.

Para a última parte consideramos $\ell = \operatorname{ord}_p(a)$ e mostraremos primeiramente, por indução sobre α, que $a^{\ell p^{\alpha-1}} = A'_\alpha p^\alpha + 1$, em que $A'_\alpha \in \mathbb{Z}$ e $p \nmid A'_\alpha$. Para $\alpha = 1$, é imediato que $a^\ell \equiv 1 \pmod{p}$. Assim, podemos escrever $a^\ell = A'_1 p + 1, A'_1 \in \mathbb{Z}$. Notamos que se $p \mid A'_1$, então $a^\ell \equiv 1 \pmod{p^2}$, o que contradiz a hipótese. Logo, $p \nmid A'_1$.

Suponhamos que o resultado vale para $\alpha > 1$. Então existe $A'_\alpha \in \mathbb{Z}$, tal que $p \nmid A'_\alpha$ e $a^{\ell p^{\alpha-1}} = A'_\alpha p^\alpha + 1$. Elevando ambos os lados à potência p, temos

$$a^{\ell p^\alpha} = \sum_{i=0}^{p} \binom{p}{i} (A'_\alpha p^\alpha)^i = 1 + p(A'_\alpha p^\alpha) + \binom{p}{2} (A'_\alpha p^\alpha)^2 + \cdots + (A'_\alpha p^\alpha)^p$$

Observamos que $\binom{p}{i}(A'_\alpha p^\alpha)^i$ é múltiplo de $p^{\alpha+2}$, para $i \geq 2$. Dessa forma, podemos escrever $a^{\ell p^\alpha} = 1 + A'_\alpha p^{\alpha+1} + Bp^{\alpha+2}$, em que $B \in \mathbb{Z}$. Logo, $a^{\ell p^\alpha} = 1 + A'_{\alpha+1} p^{\alpha+1}$, em que $A'_{\alpha+1} = A'_\alpha + Bp$. Com isso, $A'_{\alpha+1} \equiv A'_\alpha \not\equiv 0 \pmod{p}$, ou seja, $p \nmid A'_{\alpha+1}$, como desejado.

Por fim, utilizaremos indução sobre α para mostrar que $\operatorname{ord}_{p^\alpha}(a) = \ell p^{\alpha-1}$. Para $\alpha = 1$ é imediato. Suponhamos que o resultado vale para $\alpha > 1$, isto é, $\operatorname{ord}_{p^\alpha}(a) = \ell p^{\alpha-1}$.

Pelo que mostramos anteriormente, a ordem módulo $p^{\alpha+1}$ se mantém a mesma que a ordem módulo p^α ou é essa multiplicada por p. Daí,

$$\mathrm{ord}_{p^{\alpha+1}}(a) \in \{\mathrm{ord}_{p^\alpha}(a), \mathrm{ord}_{p^\alpha}(a)p\} = \{\ell p^{\alpha-1}, \ell p^\alpha\}.$$

Vimos que $a^{\ell p^{\alpha-1}} = A'_\alpha p^\alpha + 1$, em que $p \nmid A'_\alpha$. Donde $a^{\ell p^{\alpha-1}} \not\equiv 1 \pmod{p^{\alpha+1}}$. Portanto, $\mathrm{ord}_{p^{\alpha+1}}(a)$ não pode ser $\ell p^{\alpha-1}$ e a demonstração está completa.

□

Observação 4.11. *Considerando as mesmas hipóteses do lema anterior, mas com d ímpar, temos, em particular, que $p_1, \ldots, p_r$ também são todos ímpares. Suponhamos que $\mathrm{ord}_{p_j}(a)$ é ímpar para todo $j \in \{1, 2, \ldots, r\}$. Assim,*

$$\mathrm{ord}_d(a) = \mathrm{mmc}(\mathrm{ord}_{p_1}(a)p_1^{\beta_1}, \ldots, \mathrm{ord}_{p_r}(a)p_r^{\beta_r})$$

também é ímpar.

Corolário 4.12. *Seja n um inteiro positivo ímpar e q uma potência de 2. Suponhamos que $\mathrm{mdc}(n, q^2-1) = \mathrm{mdc}(n, q-1)$. Se (n, q) é 3-sparse, então (n, q^2) também o é.*

Demonstração. Seja p um primo que divide n. Então, pelo Exemplo 4.5, (p, q) é 3-sparse. Pelo Lema 4.9, segue que $t = \mathrm{ord}_p(q)$ é ímpar ou 2. Suponhamos que $t = 2$. Assim,

$$t = 2 \implies q^2 \equiv 1 \pmod{p} \implies p \mid q^2 - 1 \implies p \mid \mathrm{mdc}(n, q^2-1).$$

Como $\mathrm{mdc}(n, q^2-1) = \mathrm{mdc}(n, q-1)$, vem que

$$p \mid \mathrm{mdc}(n, q-1) \implies p \mid q-1 \implies q \equiv 1 \pmod{p}.$$

O que contradiz $t = \mathrm{ord}_p(q) = 2$. Dessa forma, t é ímpar.

Seja d um divisor de n. Observamos que d é ímpar e, pelo que acabamos de fazer e a Observação 4.10, segue que $t_d = \mathrm{ord}_d(q)$ também é ímpar. Além disso, posto $t'_d = \mathrm{ord}_d(q^2)$, vale que

$$q^{2t'_d} \equiv 1 \pmod{d} \implies t_d \mid 2t'_d \implies t_d \mid t'_d.$$

Também, $(q^2)^{t_d} \equiv 1 \pmod{p}$ implica que t'_d divide t_d. Logo, $t_d = t'_d$. Ou seja, $\mathrm{ord}_d(q) = \mathrm{ord}_d(q^2)$.

Além disso, como $x^n - 1 = \prod_{d|n}(x)$ e cada $\Phi_d(x)$ se fatora em $\varphi(d)/t_d$ polinômios irredutíveis de grau t_d sobre $\mathbb{F}_q$ e $\mathbb{F}_{q^2}$ (Teorema 1.25), segue que $x^n - 1$ se fatora na mesma quantidade de polinômios sobre $\mathbb{F}_q$ e $\mathbb{F}_{q^2}$. Isso mostra que a fatoração é a mesma sobre esses dois corpos.

Em particular, se (n, q) é 3-sparse, então (n, q^2) também o é. □

Agora estamos prontos para caracterizar os inteiros positivos n, tais que $(n, 2)$ é 3-sparse.

Teorema 4.13. *Seja $n > 1$ um inteiro ímpar. O par $(n, 2)$ é 3-sparse se, e somente se, $n = 3^k$ ou $n = 7^k$, para algum inteiro positivo k. Além disso, temos as seguintes fatorações sobre $\mathbb{F}_2$:*

(i) $\Phi_{3^k}(x) = (x^{2\cdot 3^{k-1}} + x^{3^{k-1}} + 1)$;

(ii) $\Phi_{7^k}(x) = (x^{3\cdot 7^{k-1}} + x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + x^{7^{k-1}} + 1)$.

Demonstração. No Exemplo 4.3 mostramos que $(3, 2)$ é 3-sparse. Seja $p > 3$ primo, $t = \mathrm{ord}_p(2)$ e suponhamos que $(p, 2)$ é 3-sparse. Como $p > 3$, segue que $t > 2$. Pelo Lema 4.9, vem que

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1 = \prod_{i=1}^{s}(x^t + x^{a_i} + 1), \tag{4.4}$$

em que os coeficientes são todos 1 pois estamos sobre $\mathbb{F}_2$ e $a_1 < a_2 < \cdots < a_s < t$ são inteiros positivos. Como $t > 2$ e $p > 3$, comparando os dois lados de (4.4), concluímos que $a_1 = 1$ e $a_2 = 2$. Em particular, $x^t + x + 1$ e $x^t + x^2 + 1$ são irredutíveis sobre $\mathbb{F}_2$. Assim, t é ímpar. De fato, se $t = 2k, k \in \mathbb{Z}$, então $(x^t + x^2 + 1) = (x^{2k} + x^2 + 1) = (x^k + x + 1)^2$, o que contradiz a irredutibilidade de $x^t + x^2 + 1$ sobre $\mathbb{F}_2$.

O polinômio recíproco de x^t+x+1 é $x^t+x^{t-1}+1$, logo, o Lema 3.19 implica que $x^t+x^{t-1}+1$ também é irredutível sobre $\mathbb{F}_2$. Suponhamos que $t \equiv 1, 7 \pmod 8$, como $2 \mid 2t$, o item (iii) do Corolário 3.17 implica que $x^t + x^2 + 1$ tem um número par de fatores irredutíveis, uma contradição com a irredutibilidade desse polinômio sobre $\mathbb{F}_2$. Logo, $t \equiv 3, 5 \pmod 8$. Além disso, $t - 1 \mid 2t$, pois, do contrário, o item (ii) do Corolário 3.17 implica que $x^t + x^{t-1} + 1$ tem um número par de fatores irredutíveis, uma contradição com a irredutibilidade desse polinômio.

Como $t > 2$ é ímpar e $t - 1 \mid 2t$, devemos ter $t = 3$. Com isso, $t = \mathrm{ord}_p(2) = 3$ e $2^3 \equiv 8 \equiv 1 \pmod p$, ou seja, $p \mid 7$. Logo, $p = 7$. Concluímos que, se p é um primo ímpar e $(p, 2)$ é 3-sparse, então $p \in \{3, 7\}$.

Consideramos agora $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \geq 1$ a fatoração do número ímpar n e suponhamos que $(n, 2)$ é 3-sparse. Para cada $j \in \{1, 2, \ldots, s\}$, é claro que p_j é ímpar e, pelo Exemplo 4.5, o par $(p_j, 2)$ é 3-sparse. Pelo que acabamos de provar, $p_j \in \{3, 7\}$ e, consequentemente, $\mathrm{rad}(n) \in \{3, 7, 21\}$. Agora lembramos que $x^n - 1 = \prod_{d|n} \Phi_d(x)$ e vamos analisar o que acontece em cada um desses três casos.

(i) $\mathrm{rad}(n) = 3$. Nesse caso, $n = 3^k$, para algum inteiro positivo k. Pelo Lema 1.27 e o Exemplo 1.29, temos

$$\Phi_{3^k}(x) = \Phi_3(x^{3^{k-1}}) = x^{2\cdot 3^{k-1}} + x^{3^{k-1}} + 1.$$

Pelo Exemplo 1.45, o polinômio acima é irredutível sobre $\mathbb{F}_2$.

(ii) $\mathrm{rad}(n) = 7$. Nesse caso, $n = 7^k$, para algum inteiro positivo k. Pelo Lema 1.27 e o Exemplo 1.30, temos

$$\Phi_{7^k}(x) = \Phi_7(x^{7^{k-1}}) = (x^{3\cdot 7^{k-1}} + x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + x^{7^{k-1}} + 1).$$

Pelo Exemplo 1.46, os polinômios $(x^{3\cdot 7^{k-1}}+x^{2\cdot 7^{k-1}}+1)$ e $(x^{3\cdot 7^{k-1}}+x^{7^{k-1}}+1)$ são irredutíveis sobre $\mathbb{F}_2$.

(iii) $\text{rad}(n) = 21$. Nesse caso, 21 é divisor de n. Pelo Exemplo 4.5, $(21, 2)$ é 3-sparse, o que é uma contradição, pois $\Phi_{21}(x)$ é um fator de $x^{21} - 1$ e, pelo Exemplo 1.30, se fatora da seguinte forma sobre $\mathbb{F}_2$:

$$\Phi_{21}(x) = (x^6 + x^4 + x^2 + x + 1)(x^6 + x^5 + x^4 + x^2 + 1).$$

Ou seja, $x^{21}-1$ possui fatores irredutíveis sobre $\mathbb{F}_2$ que não são binômios e nem trinômios. Logo, $\text{rad}(n) = 21$ não pode acontecer.

Isso prova que, se $(n, 2)$ é 3-sparse, então $n \in \{3^k, 7^k\}$, para algum inteiro positivo k.

Para a recíproca, basta observar que

$$x^{3^k} - 1 = \prod_{d|3^k} \Phi_d(x) = \prod_{m=0}^{k} \Phi_{3^m}(x) \quad \text{e} \quad x^{7^k} - 1 = \prod_{d|7^k} \Phi_d(x) = \prod_{m=0}^{k} \Phi_{7^m}(x).$$

Em ambos os casos provamos que os polinômios $\Phi_{3^m}(x)$ e $\Phi_{7^m}(x)$ se fatoram em trinômios para $m \geq 1$, e para $m = 0$ temos $\Phi_1(x) = x - 1$. Portanto, $(3^k, 2)$ e $(7^k, 2)$ são 3-sparse para todo inteiro positivo k. □

Agora vamos prosseguir para a caracterização dos pares $(n, 4)$ que são 3-sparse. Os próximos dois resultados são cruciais para isso.

Lema 4.14. *Sejam $p > 7$ um número primo, $t = \text{ord}_p(4)$ e suponhamos que o par $(p, 4)$ é 3-sparse. Então todo fator irredutível de $\Phi_p(x)$ sobre $\mathbb{F}_2$ é igual a algum dos pentanômios dados no Lema 4.8.*

Demonstração. Como $p > 7$, temos $t > 2$. Como 4 é uma potência par de 2, o Lema 4.9 implica que t é ímpar e todos os fatores irredutíveis de $\Phi_p(x)$ sobre $\mathbb{F}_4$ são trinômios.

De $t = \text{ord}_p(4)$, temos $4^t \equiv 1 \pmod{p}$ e, consequentemente, $2^{2t} \equiv 1 \pmod{p}$. Assim, $s = \text{ord}_p(2)$ divide $2t$. Pela Proposição 1.16, segue que

$$t = \text{ord}_p(4) = \text{ord}_p(2^2) = \frac{s}{\text{mdc}(2, s)}.$$

Suponhamos que s é ímpar, então

$$t = \text{ord}_p(4) = \frac{s}{\text{mdc}(2, s)} = s.$$

Aplicando o Teorema 1.25 como fizemos na demonstração do Corolário 4.12, segue que a fatoração de $\Phi_p(x)$ sobre $\mathbb{F}_2$ e $\mathbb{F}_4$ é a mesma. Assim, o par $(p, 2)$ também é 3-sparse. Como $p > 7$, isso contradiz o Teorema 4.13. Logo, s é par e

$$t = \text{ord}_p(4) = \frac{s}{\text{mdc}(2, s)} = \frac{s}{2} \implies s = 2t.$$

Novamente pelo Teorema 1.25, cada fator irredutível de $\Phi_p(x)$ sobre $\mathbb{F}_2$ tem grau $2t$ e, consequentemente, se fatora em dois trinômios de grau t sobre $\mathbb{F}_4$.

O resultado segue pelo Lema 4.8. □

Para a proposição a seguir vamos utilizar alguns dos pentanômios apresentados no Lema 4.8. Lembramos que eles são irredutíveis sobre $\mathbb{F}_2$ e têm as seguintes fatorações sobre $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$:

Exemplo 4.15. *Sobre $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, temos*

(i) $F_{1,t}(x) = x^{2t} + x^{t+1} + x^2 + x + 1 = (x^t + \alpha x + 1)(x^t + \alpha^2 x + 1)$;

(ii) $F_{2,t}(x) = x^{2t} + x^{t+2} + x^4 + x^2 + 1 = (x^t + \alpha x^2 + 1)(x^t + \alpha^2 x^2 + 1)$;

(iii) $F_{3,t}(x) = x^{2t} + x^{t+3} + x^6 + x^3 + 1 = (x^t + \alpha x^3 + 1)(x^t + \alpha^2 x^3 + 1)$;

(iv) $G_{1,t}(x) = x^{2t} + x^{t+1} + x^2 + x^t + 1 = (x^t + \alpha x + \alpha)(x^t + \alpha^2 x + \alpha^2)$;

(v) $H_{1,t}(x) = x^{2t} + x^t + x^2 + x + 1 = (x^t + x + \alpha)(x^t + x + \alpha^2)$;

(vi) $H_{2,t}(x) = x^{2t} + x^t + x^4 + x^2 + 1 = (x^t + x^2 + \alpha)(x^t + x^2 + \alpha^2)$;

(vii) $H_{3,t}(x) = x^{2t} + x^t + x^6 + x^3 + 1 = (x^t + x^3 + \alpha)(x^t + x^3 + \alpha^2)$.

Quando escrevemos LHS (RHS) de uma equação estamos nos referindo ao lado esquerdo (direito) dessa equação. Utilizaremos essa abreviação adiante.

Proposição 4.16. *Sejam $p > 7$ um número primo e $t = \mathrm{ord}_p(4)$. Suponhamos que $(p, 4)$ é 3-sparse. Então um dos polinômios $F_{3,t}(x), H_{3,t}(x)$ divide $\Phi_p(x)$ e $t \equiv 0 \pmod 3$.*

Demonstração. Pelo lema anterior, existem conjuntos $A, B, C \subset \mathbb{N}$, tais que

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1 = \left(\prod_{a\in A} F_{a,t}(x)\right)\left(\prod_{b\in B} G_{b,t}(x)\right)\left(\prod_{c\in C} H_{c,t}(x)\right). \tag{4.5}$$

A fim de obter informações sobre os conjuntos A, B e C, vamos comparar os monômios que aparecem em ambos os lados de (4.5). Como $p > 7$, temos $t > 3$ e os monômios x, x^2 e x^3 aparecem em LHS de (4.5), então o mesmo deve acontecer em RHS. Observamos que somente $F_{1,t}(x)$ e $H_{1,t}(x)$ possuem o monômio x, logo, $1 \in A \cup C$. Mas o produto $F_{1,t}(x)H_{1,t}(x)$ não possui esse monômio, donde $1 \notin A \cap C$. Assim, somente um entre $F_{1,t}(x)$ e $H_{1,t}(x)$ aparece em RHS, ou seja, o monômio x aparece apenas uma vez. Isso implica que o monômio x^2 não aparece em RHS como produto $x \cdot x$, logo, x^2 deve aparecer em algum dos pentanômios.

Além disso, notamos que o termo x^2 não aparece em RHS ao fazer o produto de dois pentanômios que possuem esse monômio. Portanto, se s denota o número de pentanômios que possuem o termo x^2, então s é ímpar. Para $t > 3$, todos os pentanômios do Lema 4.8 que possuem x^2 são

$$\{F_{1,t}(x), F_{2,t}(x), G_{1,t}(x), H_{1,t}(x), H_{2,t}(x)\}.$$

Notamos que $F_{1,t}(x)$ e $H_{1,t}(x)$ não podem aparecer simultaneamente em RHS, pois $1 \notin A \cap C$. Então $s < 5$, ou seja, $s \in \{1, 2\}$. Vamos analisar essas duas possibilidades.

(i) $s = 1$. Como $1 \in A \cup C$, temos duas possibilidades para esse conjunto de pentanômios: $\{F_{1,t}(x)\}$ e $\{H_{1,t}(x)\}$. Em ambos os casos, o monômio x^3 não é "gerado" pelo produto $x \cdot x^2$, pois temos apenas um pentanômio em RHS com os monômios x e x^2 simultaneamente. Ou seja, um pentanômio com o termo x^3 deve aparecer em RHS. Como $t > 3$, temos exatamente duas possibilidades para esse pentanômio: $F_{3,t}(x)$ e $H_{3,t}(x)$.

(ii) $s = 3$. Como $1 \in A \cup C$ e $1 \notin A \cap C$, temos novamente duas possibilidades: pegamos um do conjunto $\{F_{1,t}(x), H_{1,t}(x)\}$ e dois do conjunto $\{F_{2,t}(x), G_{1,t}(x), H_{2,t}(x)\}$. Novamente, o termo x^3 não aparece ao multiplicar esses pentanômios e, como no caso anterior, $F_{3,t}(x)$ ou $H_{3,t}(x)$ deve aparecer em RHS.

Em ambos os casos, $F_{3,t}(x)$ ou $H_{3,t}(x)$ divide $\Phi_p(x)$.

Para a segunda parte notamos que, para $\alpha \in \mathbb{F}_4 = \mathbb{F}_2(\alpha)$, vale que

$$\alpha^3 = \alpha^2\alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha = (\alpha + 1) + \alpha = 1,$$

daí,

$$\begin{aligned} F_{3,t}(\alpha) &= \alpha^{2t} + \alpha^{t+3} + \alpha^6 + \alpha^3 + 1 \\ &= \alpha^{2t} + \alpha^t\alpha^3 + (\alpha^3)^2 + \alpha^3 + 1 \\ &= \alpha^{2t} + \alpha^t + 1 + 1 + 1 \\ &= \alpha^{2t} + \alpha^t + 1, \end{aligned}$$

e também

$$H_{3,t}(\alpha) = \alpha^{2t} + \alpha^t + \alpha^6 + \alpha^3 + 1 = \alpha^{2t} + \alpha^t + 1 + 1 + 1 = \alpha^{2t} + \alpha^t + 1.$$

Ou seja, $H_{3,t}(\alpha) = F_{3,t}(\alpha) = \alpha^{2t} + \alpha^t + 1$.

Suponhamos que $t \not\equiv 0 \pmod 3$, então $t \equiv 1, 2 \pmod 3$. Vamos analisar essas duas possibilidades.

(i) $t \equiv 1 \pmod 3$. Nesse caso, $t = 3\ell + 1, \ell \in \mathbb{Z}$ e

$$\begin{aligned} H_{3,t}(\alpha) = F_{3,t}(\alpha) &= \alpha^{2t} + \alpha^t + 1 \\ &= \alpha^{6\ell+2} + \alpha^{3\ell+1} + 1 \\ &= (\alpha^6)^\ell\alpha^2 + \alpha^{3\ell}\alpha + 1 \\ &= \alpha^2 + \alpha + 1 \\ &= 0. \end{aligned}$$

(ii) $t \equiv 2 \pmod 3$. Nesse caso, $t = 3\ell + 2, \ell \in \mathbb{Z}$ e

$$\begin{aligned} H_{3,t}(\alpha) = F_{3,t}(\alpha) &= \alpha^{2t} + \alpha^t + 1 \\ &= \alpha^{6\ell+4} + \alpha^{3\ell+2} + 1 \\ &= (\alpha^6)^\ell \alpha^3 \alpha + \alpha^{3\ell}\alpha^2 + 1 \\ &= \alpha + \alpha^2 + 1 \\ &= 0. \end{aligned}$$

Em ambos os casos, α é uma raiz de $H_{3,t}(x)$ e de $F_{3,t}(x)$ $\mathbb{F}_4$. Consequentemente, $(x - \alpha)$ divide esses dois pentanômios sobre $\mathbb{F}_4$, o que contradiz o fato de que eles se fatoram em exatamente dois trinômios irredutíveis em $\mathbb{F}_4[x]$. Portanto, $t \equiv 0 \pmod 3$. □

Agora sim podemos caracterizar os pares $(n, 4)$ que são 3-sparse.

Teorema 4.17. *Seja $n > 1$ um inteiro ímpar. O par $(n, 4)$ é 3-sparse se, e somente se, n tem alguma das seguintes formas:*

$$3^k, 5^k, 7^k, 3^m \cdot 5^k, 3 \cdot 7^k,$$

em que m e k são inteiros positivos. Além disso, para $\alpha \in \mathbb{F}_4 = \mathbb{F}_2(\alpha)$ temos as seguintes fatorações sobre $\mathbb{F}_4$:

(i) $\Phi_{3^k}(x) = (x^{3^{k-1}} + \alpha)(x^{3^{k-1}} + \alpha^2)$;

(ii) $\Phi_{5^k}(x) = (x^{2\cdot 5^{k-1}} + \alpha x^{5^{k-1}} + 1)(x^{2\cdot 5^{k-1}} + \alpha^2 x^{5^{k-1}} + 1)$;

(iii) $\Phi_{7^k}(x) = (x^{3\cdot 7^{k-1}} + x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + x^{7^{k-1}} + 1)$;

(iv) $\Phi_{3^m\cdot 5^k}(x) = \prod_{i=1}^{2}(x^{2\cdot 3^{m-1}\cdot 5^{k-1}} + x^{3^{m-1}\cdot 5^{k-1}} + \alpha^i)(x^{2\cdot 3^{m-1}\cdot 5^{k-1}} + \alpha^i x^{3^{m-1}\cdot 5^{k-1}} + \alpha^i)$;

(v) $\Phi_{3\cdot 7^k}(x) = \prod_{i=1}^{2}(x^{3\cdot 7^{k-1}} + \alpha^i x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + \alpha^i x^{7^{k-1}} + 1)$.

Demonstração. Sejam $p > 7$ primo, $t = \mathrm{ord}_p(4)$ e suponhamos que $(p, 4)$ é 3-sparse. Pela Proposição 4.16, $F_{3,t}(x)$ ou $H_{3,t}(x)$ divide $\Phi_p(x)$ e $t \equiv 0 \pmod 3$. Assim, podemos escrever $t = 3\ell$, em que ℓ é um inteiro positivo. Como $F_{3,t}(x)$ ou $H_{3,t}(x)$ divide $\Phi_p(x)$, analisando as fatorações desses pentanômios no Exemplo 4.15, concluímos que $x^{3\ell} + ax^3 + b$ é um fator irredutível de $\Phi_p(x)$ sobre $\mathbb{F}_4$.

Consideramos $f(x) = x^\ell + ax + b$ e suponhamos que esse polinômio é redutível sobre $\mathbb{F}_4$. Então $f(x) = g(x)h(x)$, em que $g(x), h(x) \in \mathbb{F}_4[x]$ e $\partial(g(x)) > 0$ ou $\partial(h(x)) > 0$. Isso implica $f(x^3) = x^{3\ell} + ax^\ell + b = g(x^3)h(x^3)$, o que é uma contradição com a irredutibilidade desse trinômio. Logo, $f(x)$ é irredutível sobre $\mathbb{F}_4$.

Observamos que $f(x^3)$ é um fator irredutível de $\Phi_p(x)$ sobre $\mathbb{F}_4$. Pelo Exemplo 1.42, segue que a ordem de $f(x^3)$ é p. Além disso, como $f(x)$ e $f(x^3)$ são irredutíveis sobre $\mathbb{F}_4$, o Teorema

1.44 implica que $p = \mathrm{ord}(f(x^3)) = 3\,\mathrm{ord}(f(x))$, donde 3 divide p. Como p é primo, segue que $p = 3$, contradizendo nossa hipótese de que $p > 7$.

Isso nos mostra que se p é um primo ímpar e $(p, 4)$ é 3-sparse, então $p \in \{3, 5, 7\}$. Se $n > 1$ é ímpar, p é um fator primo de n e $(n, 4)$ é 3-sparse, então, pelo Exemplo 4.5, o par $(p, 4)$ também é 3-sparse e, pelo que acabamos de fazer, $p \in \{3, 5, 7\}$. Segue então que $\mathrm{rad}(n) \in \{3, 5, 7, 15, 21, 35, 105\}$. Vamos analisar cada um desses casos.

(i) $\mathrm{rad}(n) = 3$. Nesse caso, $n = 3^k$, para algum inteiro positivo k. Pelo Exemplo 1.31 e o Lema 1.27, temos

$$\Phi_{3^k}(x) = (x^{3^{k-1}} + \alpha)(x^{3^{k-1}} + \alpha^2).$$

Pelo item (i) do Exemplo 1.47, essa é a fatoração de $\Phi_{3^k}(x)$ sobre $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$.

(ii) $\mathrm{rad}(n) = 5$. Nesse caso, $n = 5^k$, para algum inteiro positivo k. Pelo Exemplo 1.31 e o Lema 1.27, temos

$$\Phi_{5^k}(x) = (x^{2\cdot 5^{k-1}} + \alpha x^{5^{k-1}} + 1)(x^{2\cdot 5^{k-1}} + \alpha^2 x^{5^{k-1}} + 1).$$

Pelo item (ii) do Exemplo 1.47, essa é a fatoração de $\Phi_{5^k}(x)$ sobre $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$.

(iii) $\mathrm{rad}(n) = 7$. Nesse caso, $n = 7^k$, para algum inteiro positivo k. Além disso, pela Proposição 1.16, temos

$$\mathrm{ord}_7(2) = 3 \quad \text{e} \quad \mathrm{ord}_7(4) = \mathrm{ord}_7(2^2) = \frac{3}{\mathrm{mdc}(2,3)} = 3.$$

Pelo Lema 4.10, isso implica que $\mathrm{ord}_{7^k}(2) = \mathrm{ord}_{7^k}(4) = 3 \cdot 7^{k-1}$. Assim, pelo Teorema 1.25, a fatoração de $\Phi_{7^k}(x)$ sobre $\mathbb{F}_2$ e $\mathbb{F}_4$ é a mesma. Pelo Teorema 4.13, segue que

$$\Phi_{7^k}(x) = (x^{3\cdot 7^{k-1}} + x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + x^{7^{k-1}} + 1)$$

é a fatoração de $\Phi_{7^k}(x)$ sobre $\mathbb{F}_4$.

(iv) $\mathrm{rad}(n) = 15$. Nesse caso, $n = 3^m \cdot 5^k$, em que m e k são inteiros positivos. Pelo Exemplo 1.31 e o Lema 1.27 (aplicado duas vezes), temos

$$\Phi_{3^m\cdot 5^k}(x) = \prod_{i=1}^{2} (x^{2\cdot 3^{m-1}\cdot 5^{k-1}} + x^{3^{m-1}\cdot 5^{k-1}} + \alpha^i)(x^{2\cdot 3^{m-1}\cdot 5^{k-1}} + \alpha^i x^{3^{m-1}\cdot 5^{k-1}} + \alpha^i).$$

Pelo item (iii) do Exemplo 1.47, essa é a fatoração de $\Phi_{3^m\cdot 5^k}(x)$ sobre $\mathbb{F}_4$.

(v) $\mathrm{rad}(n) = 21$. Nesse caso, $n = 3^m \cdot 7^k$, em que m e k são inteiros positivos. Para $m = 1$, o

Lema 1.27 e o Exemplo 1.31, implicam que

$$\Phi_{3\cdot 7^k}(x) = \prod_{i=1}^{2}(x^{3\cdot 7^{k-1}} + \alpha^i x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + \alpha^i x^{7^{k-1}} + 1).$$

Pelo item (iv) do Exemplo 1.47, essa é a fatoração de $\Phi_{3\cdot 7^k}(x)$ sobre $\mathbb{F}_4$. No entanto, para $m \geq 2$, segue que 63 divide n e, consequentemente, $\Phi_{63}(x)$ divide $x^n - 1$. No Exemplo 1.31 mostramos que $\Phi_{63}(x)$ possui fatores irredutíveis sobre $\mathbb{F}_4$ que não são binômios e nem trinômios. Isso implica que $(3^m \cdot 7^k, 4)$ não é 3-sparse para $m \geq 2$.

(vi) $\mathrm{rad}(n) = \{35, 105\}$. Em ambos os casos, 35 divide n e, sendo assim, $\Phi_{35}(x)$ divide $x^n - 1$. No Exemplo 1.31 mostramos que $\Phi_{35}(x)$ possui fatores irredutíveis sobre $\mathbb{F}_4$ que não são binômios e nem trinômios. Isso implica que $(n, 4)$ não é 3-sparse nos casos em que $\mathrm{rad}(n) \in \{35, 105\}$.

Isso prova que se $(n, 4)$ é 3-sparse, então $n \in \{3^k, 5^k, 7^k, 3^m \cdot 5^k, 3 \cdot 7^k\}$.

Para a recíproca, observamos que as fatorações de $\Phi_{3^k}(x), \Phi_{5^k}(x), \Phi_{7^k}(x), \Phi_{3^m \cdot 5^k}(x)$ e $\Phi_{3\cdot 7^k}(x)$ se dão em binômios e trinômios e prosseguimos de forma análoga ao que fizemos no Teorema 4.13. □

Referências Bibliográficas

[1] F. E. Brochero-Martinez, C. R. Giraldo Vergara, L. de Oliveira. *Explicit factorization of* $x^n - 1 \in \mathbb{F}_q$. Designs, Codes and Cryptography, Vol. 77, No. 1, pp. 277–286, 2015. Disponível em https://doi.org/10.1007/s10623-014-0005-y.

[2] B. Chen, L. Li, R. Tuerhong. *Explicit factorization of* $x^{2^m p^n} - 1$ *over a finite field*. Finite Fields and Their Applications, Vol. 24, pp. 95–104, 2013. Disponível em https://doi.org/10.1016/j.ffa.2013.06.002.

[3] K. Cheng. *The 3-sparsity of* $X^n - 1$ *over finite fields*. arXiv preprint, arXiv:2507.06655v2, 2025. Disponível em https://doi.org/10.48550/arXiv.2507.06655.

[4] K. Cheng. *The 3-sparsity of* $X^n - 1$ *over finite fields*. arXiv preprint, arXiv:2507.10779v1, 2025. Disponível em https://doi.org/10.48550/arXiv.2507.10779.

[5] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta function*. Segunda Edição. New York: Springer-Verlag, 1984. Disponível em https://doi.org/10.1007/978-1-4612-1112-9.

[6] F. Q. Gouvêa. *p-adic Numbers: An Introduction*. Segunda Edição. New York: Springer-Verlag, 1997. Disponível em https://doi.org/10.1007/978-3-642-59058-0.

[7] S. Lang. *Algebra*. Terceira Edição. New York: Springer Science+Business Media, 2012. Disponível em https://doi.org/10.1007/978-1-4613-0041-0.

[8] R. Lidl, H. Niederreiter. *Finite Fields*. Segunda Edição. Cambridge: Cambridge University Press, 1997. Disponível em https://doi.org/10.1017/CBO9780511525926.

[9] E. L. Lima. *Espaços Métricos*. Segunda Edição. Rio de Janeiro: IMPA, CNPq , 1983.

[10] D. Oliveira, L. Reis. *On polynomials* $x^n - 1$ *over binary fields whose irreducible factors are binomials and trinomials*. Finite Fields and Their Applications, Vol. 73, 101837, 2021. Disponível em https://doi.org/10.1016/j.ffa.2021.101837.

[11] J. P. O. Santos. *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 2007.

[12] SageMath. *SageMath: Open-Source Mathematical Software System*. 2024. Disponível em: <http://www.sagemath.org>.

[13] R. G. Swan. *Factorization of polynomials over finite fields.* Pacific Journal of Mathematics, Vol. 12, No. 3, pp. 1099–1106, 1962. Disponível em https://doi.org/10.2140/pjm.1962.12.1099.

[14] J. H. Van Lint.*Introduction to Coding Theory.* Terceira Edição. New York: Springer, 1998. Disponível em https://doi.org/10.1007/978-3-642-58575-3.

[15] U. Vishne. *Factorization of trinomials over Galois fields of characteristic 2.* Finite Fields and Their Applications, Vol. 3, No. 4, pp. 370–377, 1997. Disponível em https://doi.org/10.1006/ffta.1997.0191.

[16] L. Wang, Q. Wang. *On explicit factors of cyclotomic polynomials over finite fields.* Designs, Codes and Cryptography, Vol. 63, No. 1, pp. 87–104, 2012. Disponível em https://doi.org/10.1007/s10623-011-9537-6.