Classes de polinômios irredutíveis de graus 3 em $\mathbb{Q}[x]$

Classes of irreducible polynomials of degree 3 in $\mathbb{Q}[x]$

Laerte Bemm
Universidade Estadual de Maringá (UEM), Departamento de Matemática, Programa de Pós-Graduação em Matemática (PMA), Maringá, PR, Brasil
https://orcid.org/0000-0002-0326-7662, lbemm2@uem.br

Priscila Costa Ferreira de Jesus Bemm
Universidade Estadual de Maringá (UEM), Departamento de Matemática, Maringá, PR, Brasil
https://orcid.org/0000-0003-1998-5973, pcfjbemm2@uem.br

Informações do Artigo

Como citar este artigo

BEMM, Laerte; BEMM, Priscila Costa Ferreira de Jesus. Classes de polinômios irredutíveis de graus 3 em $\mathbb{Q}[x]$. **REMAT: Revista Eletrônica da Matemática**, Bento Gonçalves, RS, v. 7, n. 1, p. e3009, 25 mar. 2021. DOI: https://doi.org/10.35819/remat2021v7i1id4212

Histórico do Artigo
Submissão: 22 de maio de 2020.
Aceite: 22 de outubro de 2020.

Palavras-chave
Polinômios de $\mathbb{Z}[x]$
Algarismo das Unidades
Critério de Irredutibilidade
Relação de Equivalência

Resumo

Neste trabalho consideramos polinômios com coeficientes inteiros e estudamos sua irredutibilidade em $\mathbb{Q}[x]$. Para isso, definimos uma relação de equivalência sobre $\mathbb{Z}[x]\backslash\{0\}$ e mostrarmos que os polinômios de grau 3 pertencentes a certas classes de equivalência são irredutíveis em $\mathbb{Q}[x]$. Mostramos também que, em alguns casos, o algarismo das unidades dos coeficientes de um polinômio determina sua classe. Finalmente, mostramos como construir polinômios irredutíveis de $\mathbb{Q}[x]$ a partir de um polinômio irredutível conhecido, acrescentando dígitos à esquerda do algarismo das unidades dos coeficientes desse polinômio.

Keywords
Polynomials in $\mathbb{Z}[x]$
Ones
Irreducibility Criterion
Equivalence Relation

Abstract

In this work we consider polynomials with integer coefficients and study the irreducibility of these polynomials in $\mathbb{Q}[x]$. We will define an equivalence relation over $\mathbb{Z}[x]\backslash\{0\}$ and we will show the polynomials of degree 3 belonging to certain equivalence classes are irreducible in $\mathbb{Q}[x]$. We will also show that, in some cases, the ones of the coefficients of a polynomial determines its class. Finally, we show how we can create irreducible polynomials from a known irreducible polynomial by adding digits to the left of the ones of the coefficients of that polynomial.

1 Introdução

Os números primos desempenham um papel crucial na Teoria dos Números. O Teorema Fundamental da Aritmética nos garante que todo número inteiro diferente de $-1, 0, 1$ pode ser escrito de modo único como produto de números primos. Além disso, é por meio deles que podemos construir os corpos finitos $\mathbb{Z}_p$s.

Em anéis de polinômios sobre domínios de integridade (em particular sobre corpos), há elementos que têm a mesma importância que os números primos têm para $\mathbb{Z}$. São os polinômios irredutíveis. É bem conhecido que todo polinômio não constante de $\mathbb{K}[x]$, em que $\mathbb{K}$ é um corpo, pode ser escrito de maneira única como produto de polinômios irredutíveis (veja o Teorema 4.14 de Hungerford, 2014). Também podemos construir corpos a partir de polinômios irredutíveis. Com efeito, se $\mathbb{K}$ é um corpo e $\langle p(x)\rangle$ é o ideal de $\mathbb{K}[x]$ gerado por um polinômio não constante, então, $p(x)$ é irredutível se e somente se o anel quociente $\dfrac{\mathbb{K}[x]}{\langle p(x)\rangle}$ é um corpo (veja o Teorema 5.10 de Hungerford, 2014). Outro resultado muito importante em Álgebra é o seguinte:

Teorema 1.1. *Se $\mathbb{K}$ é um corpo e $\langle p(x)\rangle$ é o ideal gerado por um polinômio irredutível $p(x)$, então, o anel quociente $\dfrac{\mathbb{K}[x]}{\langle p(x)\rangle}$ é uma extensão do corpo $\mathbb{K}$ que contém uma raiz de $p(x)$.*

A demonstração do resultado anterior pode ser encontrada na página 137 de Hungerford (2014).

Apesar da importância dos polinômios irredutíveis, pode ser muito difícil decidir a irredutibilidade de um polinômio dado. Há casos em que essa decisão é fácil. Por exemplo, os únicos polinômios irredutíveis de $\mathbb{C}[x]$ são os de grau 1 (veja o Corolário 4.27 de Hungerford, 2014). Para $\mathbb{R}[x]$, temos que os únicos polinômios irredutíveis são os de grau 1 e os de grau 2 $ax^2 + bx + c$ que satisfazem $b^2 - 4ac < 0$. Porém, para polinômios de $\mathbb{Q}[x]$, a dificuldade, em geral, é muito maior, pois não há uma classificação como em $\mathbb{C}[x]$ e $\mathbb{R}[x]$. Algo que ajuda muito no estudo de polinômios irredutíveis de $\mathbb{Q}[x]$ é o seguinte: *se $p(x) \in \mathbb{Q}[x]$, então, $cp(x) \in \mathbb{Z}[x]$, onde c é o mínimo múltiplo comum dos denominadores dos coeficientes de $p(x)$*. Assim, estudar a irredutibilidade de polinômios de $\mathbb{Q}[x]$ se reduz a considerar aqueles que têm coeficientes inteiros. Por isso, nesse trabalho, sempre consideramos polinômios de $\mathbb{Z}[x]$ e estudamos a irredutibilidade destes em $\mathbb{Q}[x]$.

Dessa forma, é importante descobrir critérios de irredutibilidade em $\mathbb{Q}[x]$. Um dos mais famosos desses é o Critério de Eisenstein: *se $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ é um polinômio não*

constante e se existe um número primo p tal que p divide $a_0, a_1, \ldots, a_{n-1}$, p não divide a_n e p^2 não divide a_0, então, $p(x)$ é irredutível em $\mathbb{Q}[x]$ (veja o Teorema 4.24 de Hungerford, 2014).

Neste trabalho queremos estudar a irredutibilidade (em $\mathbb{Q}[x]$) de polinômios de grau 3 com coeficientes inteiros. Para tanto, dividimo-lo em seções. Na seção 2 a seguir, fixamos algumas notações e apresentamos definições e resultados bem conhecidos. Além disso, para cada inteiro positivo m, nós definimos uma relação de equivalência sobre $\mathbb{Z}[x]\backslash\{0\}$ que será muito útil para nossos propósitos. Na seção 3 nós descrevemos todos os polinômios mônicos de grau 3 que são irredutíveis em $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ e $\mathbb{Z}_5[x]$. Com isso, podemos apresentar as classes de equivalência (da relação mencionada acima) cujos polinômios são todos irredutíveis. Vamos mostrar também que (em alguns casos) uma vez descoberto um polinômio irredutível de alguma dessas classes, novos polinômios irredutíveis podem ser construídos pelo simples "acréscimo" ou "eliminação" de dígitos a esquerda do algarismo das unidades dos seus coeficientes. Na seção 4, nós agrupamos certas classes (que chamamos de classes irredutíveis) e analisamos a irredutibilidade, em $\mathbb{Q}[x]$, de polinômios de grau 3 com coeficientes inteiros não negativos.

2 Preliminares

Nesta seção apresentamos alguns conceitos e resultados conhecidos sobre polinômios, bem como fixar algumas notações e nomenclaturas que usaremos no decorrer desse texto.

Sempre que nos referirmos aos números inteiros, vamos considerá-los na base 10 e usaremos a notação clássica $\alpha_k \cdots \alpha_0$ ou $-\alpha_k \cdots \alpha_0$, com $\alpha_k, \ldots, \alpha_0 \in \{0, 1, \ldots, 9\}$ e $\alpha_k \neq 0$, para denotar um elemento de $\mathbb{Z}$. Se um número inteiro a tem o algarismo das unidades igual a a_0, diremos que a *termina* com a_0. Por exemplo, 37.846 e $-8.970.351$ terminam com 6 e 1, respectivamente. Mais ainda, neste trabalho, fixado um inteiro positivo m, $\bar{a}$ denotará a classe de equivalência do inteiro a módulo m e $\mathbb{Z}_m$ denotará o conjunto das classes de equivalência módulo m.

Definição 2.1. *Seja $\mathbb{A}$ é um domínio de integridade. Um polinômio não nulo $p(x) \in \mathbb{A}[x]$ é irredutível se: (i) $p(x)$ não for invertível em $\mathbb{A}[x]$ e (ii) se $p(x) = f(x)g(x)$, com $f(x), g(x) \in \mathbb{A}[x]$, então, $f(x)$ ou $g(x)$ é invertível em $\mathbb{A}[x]$.*

Um polinômio não invertível é *redutível* se não for irredutível. Dessa forma, o polinômio $6x + 3 = 3(2x + 1)$ é redutível em $\mathbb{Z}[x]$, mas é irredutível em $\mathbb{Q}[x]$. Os polinômios invertíveis e o polinômio nulo não são redutíveis e nem irredutíveis.

Para polinômios de grau 3 sobre um corpo, temos o seguinte resultado, cuja demonstração pode ser encontrada em Hungerford (2014, p. 109).

Teorema 2.2. *Sejam $\mathbb{K}$ um corpo e $p(x) \in \mathbb{K}[x]$ de grau 2 ou 3. então, $p(x)$ é redutível em $\mathbb{K}[x]$ se e somente se $p(x)$ tem uma raiz em $\mathbb{K}$.*

Observação 2.3. *Sejam $f(x) = \frac{a_n}{b_n}x^n + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0} \in \mathbb{Q}[x]$ e $b = mmc(b_n, \ldots, b_1, b_0)$. então, o polinômio $bf(x) \in \mathbb{Z}[x]$ e $f(x)$ é irredutível em $\mathbb{Q}[x]$ se e somente se $bf(x)$ é irredutível em $\mathbb{Q}[x]$. Assim, para estudarmos a irredutibilidade em $\mathbb{Q}[x]$, basta considerarmos polinômios com coeficientes em $\mathbb{Z}$. Por isso, daqui em diante considerarmos apenas polinômios com coeficientes inteiros e vamos estudar a irredutibilidade destes em $\mathbb{Q}[x]$.*

Sejam $f(x) = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$, com $a_n \neq 0$ e $m \in \mathbb{Z}$ um inteiro positivo. Denotamos por $\bar{f}_m(x)$ o polinômio

$$\bar{f}_m(x) = \bar{a}_nx^n + \cdots + \bar{a}_1x + \bar{a}_0 \in \mathbb{Z}_m[x].$$

Note que se r_i denota o resto da divisão de a_i por m, para todo $i = 0, 1, \ldots, n$, então,

$$\bar{f}_m(x) = \bar{r}_nx^n + \cdots + \bar{r}_1x + \bar{r}_0 \in \mathbb{Z}_m[x].$$

Nesse caso, dizemos que $f(x)$ é do *tipo* $(r_n, \ldots, r_1, r_0)$ *módulo* m. Note que o tipo de um polinômio não nulo é definido pelo seu grau e pelos restos das divisões dos seus coeficientes por m.

Exemplo 2.4. *Para o polinômio $f(x) = x^4 - 4x^2 - 2 \in \mathbb{Z}[x]$, temos:*

- $\bar{f}_2(x) = x^4 - \bar{4}x^2 - \bar{2} = x^4 \in \mathbb{Z}_2[x]$ *e $f(x)$ é do tipo $(1, 0, 0, 0, 0)$ módulo 2;*
- $\bar{f}_3(x) = x^4 - \bar{4}x^2 - \bar{2} = x^4 + \bar{2}x^2 + \bar{1} \in \mathbb{Z}_3[x]$ *e $f(x)$ é do tipo $(1, 0, 2, 0, 1)$ módulo 3;*
- $\bar{f}_4(x) = x^4 - \bar{4}x^2 - \bar{2} = x^4 + \bar{2} \in \mathbb{Z}_4[x]$ *e $f(x)$ é do tipo $(1, 0, 0, 0, 2)$ módulo 4;*
- $\bar{f}_5(x) = x^4 - \bar{4}x^2 - \bar{2} = x^4 + x^2 + \bar{3} \in \mathbb{Z}_5[x]$ *e $f(x)$ é do tipo $(1, 0, 1, 0, 3)$ módulo 5.*

Definição 2.5. *Seja m um inteiro positivo. Dizemos que dois polinômios $f(x), g(x) \in \mathbb{Z}[x]\backslash\{0\}$ são congruentes módulo m se e somente se $f(x)$ e $g(x)$ são do mesmo tipo módulo m. Nesse caso, escrevemos $f(x) \equiv g(x) \, mod \, m$.*

É fácil ver que $\equiv$ é uma relação de equivalência. A classe de todos os polinômios de tipo $(r_n, \ldots, r_1, r_0)$ módulo m é denotada por $\overline{(r_n, \ldots, r_1, r_0)}$. Como todos os polinômios de uma classe $\overline{(r_n, \ldots, r_1, r_0)}$ tem o mesmo grau, dizemos que esse também é o *grau da classe*. Uma classe $\overline{(r_n, \ldots, r_1, r_0)}$ módulo m é dita ser *irredutível*, se o polinômio $\bar{r}_n x^n + \cdots + \bar{r}_1 x + \bar{r}_0 \in \mathbb{Z}_m[x]$ é irredutível em $\mathbb{Z}_m[x]$.

Por exemplo, a classe $\overline{(0,0,0,0)}$ é formada pelos polinômios de grau 3 cujos coeficientes são todos múltiplos de m. Mais ainda, as classes dos polinômios constantes são $\overline{(m-1)}, \ldots, \overline{(1)}$ e $\overline{(0)}$.

Para determinarmos a qual classe módulo m um polinômio $f(x) \in \mathbb{Z}[x]$ pertence, é muito útil conhecermos um critério de divisibilidade por m, pois por meio dele podemos determinar os restos das divisões dos coeficientes de $f(x)$ por m.

Pelo Critério de Divisibilidade por 2, temos que o resto da divisão $a \in \mathbb{Z}$ por 2 é

0 se e somente a terminar com $0, 2, 4, 6$ ou 8;

1 se e somente a terminar com $1, 3, 5, 7$ ou 9.

Isso significa que o algarismo das unidades de a determina o resto da divisão de a por 2.

Algo semelhante acontece para 5, pois pelo Critério de Divisibilidade por 5, temos:

(i) se $a \in \mathbb{Z}$ e $a \geq 0$, então, o resto da divisão de a por 5 é

0 se e somente a terminar com 0 ou 5;

1 se e somente a terminar com 1 ou 6;

2 se e somente a terminar com 2 ou 7;

3 se e somente a terminar com 3 ou 8;

4 se e somente a terminar com 4 ou 9.

(ii) se $a \in \mathbb{Z}$ e $a < 0$, então, o resto da divisão de a por 5 é

0 se e somente a terminar com 0 ou 5;

1 se e somente a terminar com 4 ou 9;

2 se e somente a terminar com 3 ou 8;

3 se e somente a terminar com 2 ou 7;

4 se e somente a terminar com 1 ou 6.

O resto da divisão de um número inteiro por 3 não depende apenas do algarismo das unidades como acontece com 2 e 5. De fato, pelo Critério de Divisibilidade por 3, o resto da divisão de um número inteiro $a = \alpha_k \cdots \alpha_1 \alpha_0$ por 3 é

0 se e somente o resto da divisão de $\alpha_k + \cdots + \alpha_1 + \alpha_0$ por 3 for 0;

1 se e somente o resto da divisão de $\alpha_k + \cdots + \alpha_1 + \alpha_0$ por 3 for 1;

2 se e somente o resto da divisão de $\alpha_k + \cdots + \alpha_1 + \alpha_0$ por 3 for 2.

Observação 2.6. *Pelo que vimos acima, dado um polinômio $f(x) \in \mathbb{Z}[x]$, para determinarmos a sua classe módulo 2 ou 5, basta analisarmos o grau de $f(x)$ e o algarismo das unidades de cada coeficiente. Para o caso 5, é preciso analisar também o sinal $(\geq 0$ ou $< 0)$ de cada coeficiente.*

Exemplo 2.7. *Se $\alpha = \alpha_k \cdots \alpha_1 7, \beta = \beta_l \cdots \beta_1 9, \gamma = \gamma_m \cdots \gamma_1 5$ e $\delta = \delta_n \cdots \delta_1 3$ são inteiros positivos, então o polinômio $f(x) = \alpha x^3 + \beta x^2 + \gamma x + \delta \in \mathbb{Z}[x]$ é do tipo $(1,1,1,1)$ módulo 2 e do tipo $(2,4,0,3)$ módulo 5, para quaisquer algarismos $\alpha_i, \beta_i, \gamma_i, \delta_i \in \{0,1,\ldots,9\}$. Isso significa que todos os polinômios de grau 3 com coeficientes positivos dessa forma pertencem à classe $\overline{(2,4,0,3)}$ módulo 5. Certamente nessa classe há outros polinômios, tais como $-\delta x^3 + \beta x^2 - \gamma x - \alpha$ e $-\delta x^3 + \beta x^2 + \gamma x + \delta$. Mais ainda, os polinômios $\pm\alpha x^3 \pm \beta x^2 \pm \gamma x \pm \delta \in \mathbb{Z}[x]$, obtidos por qualquer combinação de $+$ e $-$, pertencem a classe $\overline{(1,1,1,1)}$ módulo 2.*

Observação 2.8. *Também destacamos que se $f(x) \in \mathbb{Z}[x]$ pertence à classe $\overline{(r_n,\ldots,r_1,r_0)}$ módulo 2 ou 5, então o "acréscimo" ou a "eliminação" de algarismo(s) à esquerda das unidades de alguns (ou todos) coeficientes produzirá novos polinômios que também pertencem a mesma classe módulos 2 ou 5, pois esses processos não alteram as unidades dos coeficientes. Por exemplo, consideremos o polinômio $f(x) = x^3 + 3x^2 - 4$. Temos que $f(x)$ pertence à classe $\overline{(1,1,0,0)}$ módulo 2 e à classe $\overline{(1,3,0,1)}$ módulo 5. Acrescentando os algarismos 3 e 7 à esquerda dos coeficientes de x^3 e x, respectivamente, temos o polinômio $g(x) = 31x^3 + 3x^2 + 70x - 4$, que também pertence às mesmas classes módulos 2 e 5. Agora, $f(x)$ pertence à classe $\overline{(1,0,0,2)}$ módulo 3 e $g(x)$ pertence à classe $\overline{(1,0,1,2)}$. Isso mostra que para o caso 3, o acréscimo ou eliminação de dígitos pode fazer com que o novo polinômio não esteja na mesma classe do polinômio original. Por outro lado, se acrescentarmos aos coeficientes um ou mais dígitos cuja soma é múltiplo de 3, então, as classes dos polinômios se mantém as mesmas. Por exemplo, se aos coeficientes de x^2 e x de $f(x)$ acrescentarmos os dígitos $4,5$ e $1,8$, respectivamente, então, obtemos o polinômio $h(x) = x^3 + 453x^2 + 180x - 4$, que pertence à classe $\overline{(1,0,0,2)}$ módulo 3.*

O próximo resultado é bem conhecido e fornece uma condição suficiente para que um polinômio de $\mathbb{Z}[x]$ seja irredutível em $\mathbb{Q}[x]$. A demonstração pode ser encontrada em Hungerford (2014, p. 118).

Teorema 2.9. *Sejam p um número primo e $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, com $a_n \neq 0$ e $p \nmid a_n$. Se $\bar{f}_p(x) \in \mathbb{Z}_p[x]$ é irredutível em $\mathbb{Z}_p[x]$, então $f(x)$ é irredutível em $\mathbb{Q}[x]$.*

Como consequência imediata, temos:

Corolário 2.10. *Seja $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ um polinômio de grau 3 que satisfaz uma das seguintes condições:*

(i) *a_3 é ímpar e $\bar{f}_2(x)$ é irredutível em $\mathbb{Z}_2[x]$;*

(ii) *a soma dos algarismos de a_3 não é múltiplo de 3 e $\bar{f}_3(x)$ é irredutível em $\mathbb{Z}_3[x]$;*

(iii) *a_3 não termina em 0 ou 5 e $\bar{f}_5(x)$ é irredutível em $\mathbb{Z}_5[x]$.*

Então, $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Em termos de classes irredutíveis, o corolário anterior é enunciado da seguinte forma:

Corolário 2.11. *Seja $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ um polinômio de grau 3 e denotemos sua classe módulos 2, 3 ou 5 por $\overline{(r_3, r_2, r_1, r_0)}$. Suponhamos que umas das seguintes condições esteja satisfeita:*

(i) *a_3 é ímpar e a classe $\overline{(r_3, r_2, r_1, r_0)}$ módulo 2 é irredutível;*

(ii) *a soma dos algarismos de a_3 não é múltiplo de 3 e a classe $\overline{(r_3, r_2, r_1, r_0)}$ módulo 3 é irredutível;*

(iii) *a_3 não termina em 0 ou 5 e a classe $\overline{(r_3, r_2, r_1, r_0)}$ módulo 5 é irredutível.*

Então, $f(x)$ é irredutível em $\mathbb{Q}[x]$.

3 Os polinômios irredutíveis de grau 3 de $\mathbb{Z}_2[x], \mathbb{Z}_3[x]$ e $\mathbb{Z}_5[x]$

Pelo que vimos na seção anterior, se soubermos quais são as classes de grau 3 que são irredutíveis módulo $2, 3$ ou 5, podemos descrever algumas classes de polinômios de graus 3 de $\mathbb{Z}[x]$

que são irredutíveis em $\mathbb{Q}[x]$. Por isso, nesta seção vamos determinar os polinômios de grau 3 de $\mathbb{Z}_2[x], \mathbb{Z}_3[x]$ e $\mathbb{Z}_5[x]$ que são irredutíveis. Para facilitar a notação, denotaremos os elementos de $\mathbb{Z}_p$ simplesmente por $0, 1, \ldots, p-1$, para $p = 2, 3, 5$.

Seja $p \in \{2, 3, 5\}$. Um polinômio de grau de 3 de $Z_p[x]$ é da forma

$$f(x) = ax^3 + bx^2 + cx + d, \text{ com } a, b, c, d \in \mathbb{Z}_p \text{ e } a \neq 0.$$

Pelo Princípio Multiplicativo de Contagem, há $(p-1)p^3$ polinômios de grau 3 em $\mathbb{Z}_p[x]$. Como queremos determinar quais destes polinômios são irredutíveis em $\mathbb{Z}_p[x]$, basta considerarmos os mônicos, pois como $\mathbb{Z}_p$ é corpo, todo polinômio não nulo pode ser transformado em um polinômio mônico, multiplicando o polinômio dado pelo inverso de seu coeficiente líder. Claramente, em $\mathbb{Z}_2[x]$ todo polinômio não nulo é mônico. Em $\mathbb{Z}_3[x]$, os polinômios de grau 3 que não são mônicos, são da forma $2x^3 + bx^2 + cx + d$. Como 2 é inverso de 2 em $\mathbb{Z}_3$, este polinômio pode ser transformado em $x^3 + (2b)x^2 + (2c)x + 2d$. Finalmente, como em $\mathbb{Z}_5$ os inversos de $2, 3$ e 4 são, respectivamente, $3, 2$ e 4, podemos transformar

$$2x^3 + bx^2 + cx + d \text{ em } x^3 + (3b)x^2 + (3c)x + 3d;$$
$$3x^3 + bx^2 + cx + d \text{ em } x^3 + (2b)x^2 + (2c)x + 2d;$$
$$4x^3 + bx^2 + cx + d \text{ em } x^3 + (4b)x^2 + (4c)x + 4d.$$

É claro que a irredutibilidade do polinômio original é equivalente a irredutibilidade do polinômio transformado. Além disso, todo polinômio com termo independente igual 0 é redutível. Portanto, precisamos apenas estudar a irredutibilidade de polinômios do tipo

$$x^3 + bx^2 + cx + d, \text{ com } b, c, d \in \mathbb{Z}_p \text{ e } d \neq 0.$$

Dessa forma, temos $(p-1)p^2$ polinômios a serem considerados. Pelo Teorema 2.2, para decidirmos quais desses são irredutíveis em $\mathbb{Z}_p[x]$, basta descobrirmos quais não tem raízes em $\mathbb{Z}_p$.

As tabelas a seguir apresentam os $(p-1)p^2$ polinômios mencionados acima, para $p = 2, 3$ e 5, e as suas raízes (se existirem). Os polinômios que não têm raízes são os irredutíveis.

Tabela 1: Raízes dos polinômios mônicos de grau 3 de $\mathbb{Z}_2[x]$.

	Polinômio	Raízes			Polinômio	Raízes
1	x^3+1	1		3	x^3+x^2+1	Não há
2	x^3+x+1	Não há		4	x^3+x^2+x+1	1

Tabela 2: Raízes dos polinômios mônicos de grau 3 de $\mathbb{Z}_3[x]$.

	Polinômio	Raízes			Polinômio	Raízes
1	x^3+1	2		10	x^3+x^2+x+2	Não há
2	x^3+2	1		11	x^3+x^2+2x+1	Não há
3	x^3+x+1	1		12	x^3+x^2+2x+2	1, 2
4	x^3+x+2	2		13	x^3+2x^2+1	Não há
5	x^3+2x+1	Não há		14	x^3+2x^2+2	2
6	x^3+2x+2	Não há		15	x^3+2x^2+x+1	Não há
7	x^3+x^2+1	1		16	x^3+2x^2+x+2	1
8	x^3+x^2+2	Não há		17	x^3+2x^2+2x+1	1, 2
9	x^3+x^2+x+1	2		18	x^3+2x^2+2x+2	Não há

Tabela 3: Raízes dos polinômios mônicos de grau 3 de $\mathbb{Z}_5[x]$.

	Polinômio	Raízes			Polinômio	Raízes
1	x^3+1	4		51	x^3+2x^2+2x+3	Não há
2	x^3+2	2		52	x^3+2x^2+2x+4	3
3	x^3+3	3		53	x^3+2x^2+3x+1	3
4	x^3+4	1		54	x^3+2x^2+3x+2	4
5	x^3+x+1	Não há		55	x^3+2x^2+3x+3	2
6	x^3+x+2	4		56	x^3+2x^2+3x+4	1
7	x^3+x+3	1		57	x^3+2x^2+4x+1	2
8	x^3+x+4	Não há		58	x^3+2x^2+4x+2	Não há
9	x^3+2x+1	Não há		59	x^3+2x^2+4x+3	1 e 3
10	x^3+2x+2	1 e 3		60	x^3+2x^2+4x+4	Não há
11	x^3+2x+3	2		61	x^3+3x^2+1	1 e 3
12	x^3+2x+4	Não há		62	x^3+3x^2+2	Não há

13	x^3+3x+1	1 e 2		63	x^3+3x^2+3	4
14	x^3+3x+2	Não há		64	x^3+3x^2+4	Não há
15	x^3+3x+3	Não há		65	x^3+3x^2+x+1	Não há
16	x^3+3x+4	3		66	x^3+3x^2+x+2	Não há
17	x^3+4x+1	3		67	x^3+3x^2+x+3	2 e 3
18	x^3+4x+2	Não há		68	x^3+3x^2+x+4	4
19	x^3+4x+3	Não há		69	x^3+3x^2+2x+1	2
20	x^3+4x+4	2		70	x^3+3x^2+2x+2	Não há
21	x^3+x^2+1	Não há		71	x^3+3x^2+2x+3	Não há
22	x^3+x^2+2	Não há		72	x^3+3x^2+2x+4	1
23	x^3+x^2+3	1 e 2		73	x^3+3x^2+3x+1	4
24	x^3+x^2+4	3		74	x^3+3x^2+3x+2	3
25	x^3+x^2+x+1	2, 3 e 4		75	x^3+3x^2+3x+3	1
26	x^3+x^2+x+2	1		76	x^3+3x^2+3x+4	2
27	x^3+x^2+x+3	Não há		77	x^3+3x^2+4x+1	Não há
28	x^3+x^2+x+4	Não há		78	x^3+3x^2+4x+2	1 e 2
29	x^3+x^2+2x+1	1		79	x^3+3x^2+4x+3	Não há
30	x^3+x^2+2x+2	4		80	x^3+3x^2+4x+4	3
31	x^3+x^2+2x+3	3		81	x^3+4x^2+1	2
32	x^3+x^2+2x+4	1		82	x^3+4x^2+2	3 e 4
33	x^3+x^2+3x+1	Não há		83	x^3+4x^2+3	Não há
34	x^3+x^2+3x+2	2		84	x^3+4x^2+4	Não há
35	x^3+x^2+3x+3	4		85	x^3+4x^2+x+1	Não há
36	x^3+x^2+3x+4	Não há		86	x^3+4x^2+x+2	Não há
37	x^3+x^2+4x+1	Não há		87	x^3+4x^2+x+3	4
38	x^3+x^2+4x+2	3		88	x^3+4x^2+x+4	1, 2 e 3
39	x^3+x^2+4x+3	Não há		89	x^3+4x^2+2x+1	3
40	x^3+x^2+4x+4	1 e 4		90	x^3+4x^2+2x+2	2
41	x^3+2x^2+1	Não há		91	x^3+4x^2+2x+3	1
42	x^3+2x^2+2	1		92	x^3+4x^2+2x+4	4
43	x^3+2x^2+3	Não há		93	x^3+4x^2+3x+1	Não há
44	x^3+2x^2+4	2 e 4		94	x^3+4x^2+3x+2	1

45	x^3+2x^2+x+1	1		95	x^3+4x^2+3x+3	3
46	x^3+2x^2+x+2	2 e 3		96	x^3+4x^2+3x+4	Não há
47	x^3+2x^2+x+3	Não há		97	x^3+4x^2+4x+1	1 e 4
48	x^3+2x^2+x+4	Não há		98	x^3+4x^2+4x+2	Não há
49	x^3+2x^2+2x+1	4		99	x^3+4x^2+4x+3	2
50	x^3+2x^2+2x+2	Não há		100	x^3+4x^2+4x+4	Não há

As tabelas 4, 5 e 6 a seguir reúnem apenas os polinômios mônicos irredutíveis de $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ e $\mathbb{Z}_5[x]$. Elas também apresentam as classes irredutíveis módulo 2, 3 e 5, respectivamente.

Tabela 4: Polinômios mônicos e classes irredutíveis de grau 3 de $\mathbb{Z}_2[x]$.

	Polinômio	Classe			Polinômio	Classe
2	x^3+x+1	$\overline{(1,0,1,1)}$		3	x^3+x^2+1	$\overline{(1,1,0,1)}$

Tabela 5: Polinômios mônicos e classes irredutíveis de grau 3 de $\mathbb{Z}_3[x]$.

	Polinômio	Classe			Polinômio	Classe
5	x^3+2x+1	$\overline{(1,0,2,1)}$		11	x^3+x^2+2x+1	$\overline{(1,1,2,1)}$
6	x^3+2x+2	$\overline{(1,0,2,2)}$		13	x^3+2x^2+1	$\overline{(1,2,0,1)}$
8	x^3+x^2+2	$\overline{(1,1,0,2)}$		15	x^3+2x^2+x+1	$\overline{(1,2,1,1)}$
10	x^3+x^2+x+2	$\overline{(1,1,1,2)}$		18	x^3+2x^2+2x+2	$\overline{(1,2,2,2)}$

Tabela 6: Polinômios mônicos e classes irredutíveis de grau 3 de $\mathbb{Z}_5[x]$.

	Polinômio	Classe			Polinômio	Classe
5	x^3+x+1	$\overline{(1,0,1,1)}$		50	x^3+2x^2+2x+2	$\overline{(1,2,2,2)}$
8	x^3+x+4	$\overline{(1,0,1,4)}$		51	x^3+2x^2+2x+3	$\overline{(1,2,2,3)}$
9	x^3+2x+1	$\overline{(1,0,2,1)}$		58	x^3+2x^2+4x+2	$\overline{(1,2,4,2)}$
12	x^3+2x+4	$\overline{(1,0,2,4)}$		60	x^3+2x^2+4x+4	$\overline{(1,2,4,4)}$
14	x^3+3x+2	$\overline{(1,0,3,2)}$		62	x^3+3x^2+2	$\overline{(1,3,0,2)}$
15	x^3+3x+3	$\overline{(1,0,3,3)}$		64	x^3+3x^2+4	$\overline{(1,3,0,4)}$
18	x^3+4x+2	$\overline{(1,0,4,2)}$		65	x^3+3x^2+x+1	$\overline{(1,3,1,1)}$
19	x^3+4x+3	$\overline{(1,0,4,3)}$		66	x^3+3x^2+x+2	$\overline{(1,3,1,2)}$

21	x^3+x^2+1	$\overline{(1,1,0,1)}$		70	x^3+3x^2+2x+2	$\overline{(1,3,2,2)}$
22	x^3+x^2+2	$\overline{(1,1,0,2)}$		71	x^3+3x^2+2x+3	$\overline{(1,3,2,3)}$
27	x^3+x^2+x+3	$\overline{(1,1,1,3)}$		77	x^3+3x^2+4x+1	$\overline{(1,3,4,1)}$
28	x^3+x^2+x+4	$\overline{(1,1,1,4)}$		79	x^3+3x^2+4x+3	$\overline{(1,3,4,3)}$
33	x^3+x^2+3x+1	$\overline{(1,1,3,1)}$		83	x^3+4x^2+3	$\overline{(1,4,0,3)}$
36	x^3+x^2+3x+4	$\overline{(1,1,3,4)}$		84	x^3+4x^2+4	$\overline{(1,4,0,4)}$
37	x^3+x^2+4x+1	$\overline{(1,1,4,1)}$		85	x^3+4x^2+x+1	$\overline{(1,4,1,1)}$
39	x^3+x^2+4x+3	$\overline{(1,1,4,3)}$		86	x^3+4x^2+x+2	$\overline{(1,4,1,2)}$
41	x^3+2x^2+1	$\overline{(1,2,0,1)}$		93	x^3+4x^2+3x+1	$\overline{(1,4,3,1)}$
43	x^3+2x^2+3	$\overline{(1,2,0,3)}$		96	x^3+4x^2+3x+4	$\overline{(1,4,3,4)}$
47	x^3+2x^2+x+3	$\overline{(1,2,1,3)}$		98	x^3+4x^2+4x+2	$\overline{(1,4,4,2)}$
48	x^3+2x^2+x+4	$\overline{(1,2,1,4)}$		100	x^3+4x^2+4x+4	$\overline{(1,4,4,4)}$

Conclusão: se um polinômio $f(x)$ de grau 3 de $\mathbb{Z}[x]$ pertence a uma das classes módulo $2, 3$ ou 5 das tabela 4, 5 ou 6, então podemos garantir que tal polinômio é irredutível em $\mathbb{Q}[x]$. Caso ele não pertença a uma dessas classes, então não podemos afirmar nada a respeito de sua irredutibilidade. Lembramos que, para determinarmos a classe módulo 2 ou 5 de um polinômio de $\mathbb{Z}[x]$, basta analisarmos o algarismo das unidades de seus coeficientes. No caso 5, também é preciso analisar o sinal dos coeficientes.

Observação 3.1. *Observamos que todos os polinômios das formas*

$$(2k+1)x^3+(2l+1)x^2+(2m)x+(2n+1) \text{ e } (2k+1)x^3+(2l)x^2+(2m+1)x+(2n+1),$$

com $k,l,m,n,\in\mathbb{Z}$, são irredutíveis em $\mathbb{Q}[x]$, pois pertencem, respectivamente, às classes $\overline{(1,0,1,1)}$ e $\overline{(1,1,0,1)}$ módulo 2. Esses são os únicos polinômios de grau 3 para os quais podemos decidir sobre a irredutibilidade em $\mathbb{Q}[x]$ usando classes módulo 2.

Exemplo 3.2. *Consideremos o polinômio $f(x)=46x^3-37x^2+139x+121\in\mathbb{Z}[x]$. Temos que $f(x)$ pertence as classes $\overline{(0,1,1,1)}$ módulo 2 e $\overline{(1,1,1,1)}$ módulo 3, que não se encontram nas tabelas 4 e 5. Finalmente, devido ao sinal e o algarismo das unidade de cada coeficiente, $f(x)$ pertence à classe $\overline{(1,3,4,1)}$ módulo 5 que está na Tabela 6. Portanto, $f(x)$ é irredutível em $\mathbb{Q}[x]$. Conforme vimos na Observação 2.8, podemos acrescentar dígitos à esquerda do algarismo das unidades dos coeficientes de $f(x)$ para obtermos novos polinômios irredutíveis em $\mathbb{Q}[x]$, pois esse processo não*

altera as classes módulo 5*. Esse é o caso de* $g(x) = 46x^3 - 1.037x^2 + 139x + 95.121$*. Note que no coeficiente de* x^2 *foram acrescentados os algarismos 1 e 0 e, no termo independente, acrescentamos os algarismos 5 e 9.*

Exemplo 3.3. *Consideremos o polinômio* $f(x) = 13x^3 + 26x^2 + 8x + 7 \in \mathbb{Z}[x]$*. Esse polinômio pertence às classes* $\overline{(1,0,0,1)}$ *módulo* 2 *e* $\overline{(1,2,2,1)}$ *módulo* 3 *que não estão nas tabelas 4 e* 5*. Agora, observamos que esse polinômio pertence à classe* $\overline{(3,1,3,2)}$ *módulo* 5*, que não se encontra na Tabela 6, pois* $f(x)$ *não é um polinômio mônico. Por isso, precisamos mudar o modo de análise. Temos que* $\bar{f}_5(x) = 3x^3 + x^2 + 3x + 2 \in \mathbb{Z}_5[x]$*. Para torná-lo mônico, multiplicamo-lo por* 2 *e obtemos* $\bar{g}_5(x) = x^3 + 2x^2 + x + 4 \in \mathbb{Z}_5[x]$*. Como esse polinômio é irredutível em* $\mathbb{Z}_5[x]$ *(veja o polinômio 48 da Tabela 6), temos que* $f(x)$ *também será em* $\mathbb{Q}[x]$*.*

Exemplo 3.4. *Vamos considerar* $f(x) = x^3 + 4x^2 + 8x + 8 \in \mathbb{Z}[x]$*. Note que ele pertence às classes* $\overline{(1,0,0,0)}$ *módulo* 2*,* $\overline{(1,1,2,2)}$ *módulo* 3 *e* $\overline{(1,4,3,3)}$ *módulo* 5 *que não se encontram nas tabelas 4, 5 e 6. Por isso, pelo método que apresentamos neste trabalho, não podemos concluir nada a respeito da sua irredutibilidade em* $\mathbb{Q}[x]$*. O Critério de Eisenstein também não se aplica. Visto que* -2 *é raiz de* $f(x)$*, obtemos que* $f(x)$ *é redutível em* $\mathbb{Q}[x]$*. Agora, acrescentando o dígito* 1 *à esquerda do termo independente* 8*, obtemos o polinômio* $g(x) = x^3 + 34x^2 + 8x + 18$*, que ainda pertence à classes* $\overline{(1,0,0,0)}$ *módulo* 2 *e* $\overline{(1,4,3,3)}$ *módulo* 5*, e pertence à classe* $\overline{(1,1,2,0)}$ *módulo* 3*. Ou seja, o método que descrevemos também não nos ajuda a decidir sobre a irredutibilidade de* $g(x)$*. Porém, pelo Critério de Eisenstein, para o primo* 2*,* $g(x)$ *é irredutível em* $\mathbb{Q}[x]$*. Por outro lado, o Critério de Eisenstein não se aplica ao polinômio* $x^3 + 3x + 9$*, mas pela Observação 3.1, tal polinômio é irredutível em* $\mathbb{Q}[x]$*. Da mesma forma, não podemos aplicar o Critério de Eisenstein para o polinômio* $x^3 + 21x^2 + 30x + 27$*. No entanto, ele pertence à classe* $\overline{(1,1,0,2)}$ *módulo* 5 *e, portanto, é irredutível em* $\mathbb{Q}[x]$*.*

Observação 3.5. *Conforme o exemplo anterior, ao acrescentarmos dígitos a esquerda do algarismo das unidades dos coeficientes de um polinômio redutível, podemos obter um polinômio irredutível. O mesmo exemplo também mostra que se retirarmos dígitos dos coeficientes de um polinômio irredutível que não pertence a alguma das classes das tabelas 4, 5 e 6, podemos obter em um polinômio redutível. Como já vimos, esses processos de acrescentar e eliminar dígitos não transformam polinômios que pertencem às classes irredutíveis módulo* 2 *ou* 5 *em polinômios redutíveis de* $\mathbb{Q}[x]$*. Finalmente, quando o Critério de Eisentein não se aplica a um polinômio, podemos determinar as classes módulo* $2, 3$ *ou* 5 *dele e verificar facilmente nas tabelas acima se alguma delas é irredutível.*

4 Aplicação em polinômios de grau 3 com coeficientes não negativos

Nesta seção, vamos nos concentrar na Tabela 6 e dividi-la em 12 conjuntos disjuntos. As classes que formam cada conjunto foram escolhidos de modo a terem duas ou três coordenadas iguais. Acreditamos que, com esse agrupamento de classes irredutíveis, ficará simples observarmos a irredutibilidade em $\mathbb{Q}[x]$ de polinômios de grau 3 com coeficientes não negativos de $\mathbb{Z}[x]$.

Seja $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$, com $a > 0$ e $b, c, d \geq 0$.

- **Conjunto A**: formado pelas classes $\overline{(1,0,1,1)}$, $\overline{(1,0,1,4)}$, $\overline{(1,0,2,1)}$ e $\overline{(1,0,2,4)}$.
  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 0 \, mod \, 5 && (b \text{ termina em } 0 \text{ ou } 5), \\ c &\equiv 1 \text{ ou } 2 \, mod \, 5 && (c \text{ termina em } 1, 2, 6 \text{ ou } 7), \\ d &\equiv 1 \text{ ou } 4 \, mod \, 5 && (d \text{ termina em } 1, 4, 6 \text{ ou } 9), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto A e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto B**: formado pelas classes $\overline{(1,0,3,2)}$, $\overline{(1,0,3,3)}$, $\overline{(1,0,4,2)}$ e $\overline{(1,0,4,3)}$.
  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 0 \, mod \, 5 && (b \text{ termina em } 0 \text{ ou } 5), \\ c &\equiv 3 \text{ ou } 4 \, mod \, 5 && (c \text{ termina em } 3, 4, 8 \text{ ou } 9), \\ d &\equiv 2 \text{ ou } 3 \, mod \, 5 && (d \text{ termina em } 2, 3, 7 \text{ ou } 8), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto B e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto C**: formado pelas classes $\overline{(1,1,0,1)}$ e $\overline{(1,1,0,2)}$.
  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 1 \, mod \, 5 && (b \text{ termina em } 1 \text{ ou } 6), \\ c &\equiv 0 \, mod \, 5 && (c \text{ termina em } 0 \text{ ou } 5), \\ d &\equiv 1 \text{ ou } 2 \, mod \, 5 && (d \text{ termina em } 1, 2, 6 \text{ ou } 7), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto C e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto D**: formado pelas classes $\overline{(1,2,0,1)}$ e $\overline{(1,2,0,3)}$.

  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 2 \, mod \, 5 && (b \text{ termina em } 2 \text{ ou } 7), \\ c &\equiv 0 \, mod \, 5 && (c \text{ termina em } 0 \text{ ou } 5), \\ d &\equiv 1 \text{ ou } 3 \, mod \, 5 && (d \text{ termina em } 1, 3, 6 \text{ ou } 8), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto D e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto E**: formado pelas classes $\overline{(1,3,0,2)}$ e $\overline{(1,3,0,4)}$.

  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 3 \, mod \, 5 && (b \text{ termina em } 3 \text{ ou } 8), \\ c &\equiv 0 \, mod \, 5 && (c \text{ termina em } 0 \text{ ou } 5,) \\ d &\equiv 2 \text{ ou } 4 \, mod \, 5 && (d \text{ termina em } 2, 4, 7 \text{ ou } 9), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto E e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto F**: formado pelas classes $\overline{(1,4,0,3)}$ e $\overline{(1,4,0,4)}$.

  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 4 \, mod \, 5 && (b \text{ termina em } 4 \text{ ou } 9), \\ c &\equiv 0 \, mod \, 5 && (c \text{ termina em } 0 \text{ ou } 5,) \\ d &\equiv 3 \text{ ou } 4 \, mod \, 5 && (d \text{ termina em } 3, 4, 8 \text{ ou } 9), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto F e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto G**: formado pelas classes $\overline{(1,1,1,3)}, \overline{(1,1,1,4)}, \overline{(1,2,1,3)}$ e $\overline{(1,2,1,4)}$.

  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 1 \text{ ou } 2 \, mod \, 5 && (b \text{ termina em } 1, 2, 6 \text{ ou } 7), \\ c &\equiv 1 \, mod \, 5 && (c \text{ termina em } 1 \text{ ou } 6), \\ d &\equiv 3 \text{ ou } 4 \, mod \, 5 && (d \text{ termina em } 3, 4, 8 \text{ ou } 9), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto G e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto H**: formado pelas classes $\overline{(1,3,1,1)}, \overline{(1,3,1,2)}, \overline{(1,4,1,1)}$ e $\overline{(1,4,1,2)}$.
  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 3 \text{ ou } 4 \, mod \, 5 && (b \text{ termina em } 3, 4, 8 \text{ ou } 9), \\ c &\equiv 1 \, mod \, 5 && (c \text{ termina em } 1 \text{ ou } 6,) \\ d &\equiv 1 \text{ ou } 2 \, mod \, 5 && (d \text{ termina em } 1, 2, 6 \text{ ou } 7), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto H e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto I**: formado pelas classes $\overline{(1,2,2,2)}, \overline{(1,2,2,3)}, \overline{(1,3,2,2)}$ e $\overline{(1,3,2,3)}$.
  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 2 \text{ ou } 3 \, mod \, 5 && (b \text{ termina em } 1, 2, 3, 6, 7, \text{ ou } 8), \\ c &\equiv 2 \, mod \, 5 && (c \text{ termina em } 2 \text{ ou } 7), \\ d &\equiv 2 \text{ ou } 3 \, mod \, 5 && (d \text{ termina em } 2, 3, 7 \text{ ou } 8), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto I e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto J**: formado pelas classes $\overline{(1,1,3,1)}, \overline{(1,1,3,4)}, \overline{(1,4,3,1)}$ e $\overline{(1,4,3,4)}$.
  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 1 \text{ ou } 4 \, mod \, 5 && (b \text{ termina em } 1, 4, 6 \text{ ou } 9), \\ c &\equiv 3 \, mod \, 5 && (c \text{ termina em } 3 \text{ ou } 8), \\ d &\equiv 1 \text{ ou } 4 \, mod \, 5 && (d \text{ termina em } 1, 4, 6 \text{ ou } 9), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto J e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto K**: formado pelas classes $\overline{(1,1,4,1)}, \overline{(1,1,4,3)}, \overline{(1,3,4,1)}$ e $\overline{(1,3,4,3)}$.
  Assim, se

$$\begin{aligned} a &\equiv 1 \, mod \, 5 && (a \text{ termina em } 1 \text{ ou } 6), \\ b &\equiv 1 \text{ ou } 3 \, mod \, 5 && (b \text{ termina em } 1, 3, 6 \text{ ou } 8), \\ c &\equiv 4 \, mod \, 5 && (c \text{ termina em } 4 \text{ ou } 9), \\ d &\equiv 1 \text{ ou } 3 \, mod \, 5 && (d \text{ termina em } 1, 3, 6 \text{ ou } 8), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto K e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

- **Conjunto L**: formado pelas classes $\overline{(1,2,4,2)}$, $\overline{(1,2,4,4)}$, $\overline{(1,4,4,2)}$ e $\overline{(1,4,4,4)}$.
  Assim, se

$$\begin{aligned} a &\equiv 1\, mod\, 5 && (a \text{ termina em } 1 \text{ ou } 6),\\ b &\equiv 2 \text{ ou } 4\, mod\, 5 && (b \text{ termina em } 2,4,7 \text{ ou } 9),\\ c &\equiv 4\, mod\, 5 && (c \text{ termina em } 4 \text{ ou } 9),\\ d &\equiv 2 \text{ ou } 4\, mod\, 5 && (d \text{ termina em } 2,4,7, \text{ ou } 9), \end{aligned}$$

  então, a classe de $f(x)$ pertence ao conjunto L e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

A seguir apresentamos uma tabela contendo um resumo desta seção e com exemplos de polinômios cujas classes pertencem aos conjuntos descritos acima. As segunda, terceira, quarta e quinta colunas indicam os possíveis algarismos das unidades que a, b, c e d devem terminar para que a classe de $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ pertença ao respectivo conjunto. Lembramos que $a > 0$ e $b, c, d \geq 0$.

Tabela 7: Conjuntos de classes módulo 5.

Conjunto	a	b	c	d	Classe	Exemplo
A	1 ou 6	0 ou 5	1, 2, 7 ou 8	1, 4, 6 ou 9	$\overline{(1,0,1,1)}$	$x^3+20x^2+146x+271$
					$\overline{(1,0,1,4)}$	$6x^3+75x^2+51x+389$
					$\overline{(1,0,2,1)}$	$6x^3+10x^2+147x+66$
					$\overline{(1,0,2,4)}$	$x^3+105x^2+52x+19$
B	1 ou 6	0 ou 5	3, 4, 8 ou 9	2, 3, 7 ou 8	$\overline{(1,0,3,2)}$	$6x^3+5x^2+18x+27$
					$\overline{(1,0,3,3)}$	$x^3+75x^2+63x+33$
					$\overline{(1,0,4,2)}$	$6x^3+15x^2+29x+22$
					$\overline{(1,0,4,3)}$	$x^3+30x^2+44x+38$
C	1 ou 6	1 ou 6	0 ou 5	1, 2, 6 ou 7	$\overline{(1,1,0,1)}$	$11x^3+x^2+10x+16$
					$\overline{(1,1,0,2)}$	$x^3+26x^2+65x+37$
D	1 ou 6	2 ou 7	0 ou 5	1, 3, 6 ou 8	$\overline{(1,2,0,1)}$	$x^3+17x^2+30x+1$
					$\overline{(1,2,0,3)}$	x^3+2x^2+5x+8
E	1 ou 6	3 ou 8	0 ou 5	2, 4, 7 ou 9	$\overline{(1,3,0,2)}$	$x^3+18x^2+15x+17$
					$\overline{(1,3,0,4)}$	$x^3+23x^2+135x+49$
F	1 ou 6	4 ou 9	0 ou 5	3, 4, 8 ou 9	$\overline{(1,4,0,3)}$	$x^3+44x^2+10x+23$
					$\overline{(1,4,0,4)}$	$6x^3+19x^2+65x+144$

G	1 ou 6	1, 2, 6 ou 7	1 ou 6	3, 4, 8 ou 9	$\overline{(1,1,1,3)}$	$x^3+16x^2+21x+18$
					$\overline{(1,1,1,4)}$	$x^3+26x^2+131x+14$
					$\overline{(1,2,1,3)}$	$x^3+117x^2+16x+18$
					$\overline{(1,2,1,4)}$	$x^3+32x^2+16x+39$
H	1 ou 6	3, 4, 8 ou 9	1 ou 6	1, 2, 6 ou 7	$\overline{(1,3,1,1)}$	$6x^3+53x^2+186x+21$
					$\overline{(1,3,1,2)}$	$x^3+78x^2+61x+32$
					$\overline{(1,4,1,1)}$	$6x^3+19x^2+11x+11$
					$\overline{(1,4,1,2)}$	$x^3+34x^2+41x+87$
I	1 ou 6	2, 3, 7 ou 8	2 ou 7	2, 3, 7 ou 8	$\overline{(1,2,2,2)}$	$6x^3+17x^2+17x+22$
					$\overline{(1,2,2,3)}$	x^3+32x^2+7x+3
					$\overline{(1,3,2,2)}$	$16x^3+23x^2+22x+27$
					$\overline{(1,3,2,3)}$	x^3+43x^2+7x+3
J	1 ou 6	1, 4, 6 ou 9	3 ou 8	1, 4, 6 ou 9	$\overline{(1,1,3,1)}$	$6x^3+31x^2+83x+21$
					$\overline{(1,1,3,4)}$	$x^3+67x^2+13x+39$
					$\overline{(1,4,3,1)}$	$6x^3+19x^2+3x+11$
					$\overline{(1,4,3,4)}$	$x^3+34x^2+43x+79$
K	1 ou 6	1, 3, 6 ou 8	4 ou 9	1, 3, 8 ou 9	$\overline{(1,1,4,1)}$	$6x^3+51x^2+64x+21$
					$\overline{(1,1,4,3)}$	$x^3+86x^2+34x+9$
					$\overline{(1,3,4,1)}$	$6x^3+13x^2+14x+11$
					$\overline{(1,3,4,3)}$	x^3+3x^2+4x+3
L	1 ou 6	2, 4, 7 ou 9	4 ou 9	2, 4, 7 ou 9	$\overline{(1,2,4,2)}$	$6x^3+32x^2+49x+22$
					$\overline{(1,2,4,4)}$	$x^3+74x^2+62x+32$
					$\overline{(1,4,4,2)}$	$6x^3+24x^2+14x+17$
					$\overline{(1,4,4,4)}$	x^3+34x^2+4x+9

Nos exemplos da Tabela 7, observamos algumas curiosidades. Por exemplo, podemos aplicar o Critério de Eisenstein (com o primo 3) para mostrar que $x^3+75x^2+63x+33$ é irredutível, ou podemos observar que ele pertence ao conjunto B. Por outro lado, o Critério de Eisenstein não se aplica para determinarmos a irredutibilidade de $x^3+74x^2+62x+32$, mas como este pertence ao conjunto H, é irredutível.

5 Conclusão

Conforme propomos no início desse trabalho, obtivemos classes de polinômios de grau 3 de $\mathbb{Z}[x]$ cujos elementos são irredutíveis em $\mathbb{Q}[x]$. Dois fatos chamam a atenção. Para determinarmos a classe módulo 2 ou 5 de um polinômio, precisamos apenas analisar o algarismo das unidades dos coeficientes desse polinômio (no caso 5 é preciso observar o sinal dos coeficientes). Ou seja, não são necessários quaisquer cálculos. O segundo é que uma vez obtido um polinômio irredutível que pertença a alguma classe irredutível módulos 2 ou 5, outros polinômios irredutíveis podem ser construídos acrescentando ou eliminando dígitos à esquerda do algarismo das unidades dos coeficientes. Dessa forma, temos um método eficaz para obtermos polinômios irredutíveis de grau 3 em $\mathbb{Q}[x]$.

Referências

HUNGERFORD, T. W. **Abstract Algebra**: An Introduction. 3. ed. Boston: Books/Coles Cengage Learning, 2014.