



Universidade Regional do Cariri - URCA  
Departamento de Matemática  
Programa de Mestrado Profissional em  
Matemática em Rede Nacional



# RESOLUÇÃO DE SISTEMAS LINEARES EM $\mathbb{Z}_m$ UTILIZANDO A REGRA DE CRAMER

Joseane Alves de Sousa

Juazeiro do Norte - CE

2023

# RESOLUÇÃO DE SISTEMAS LINEARES EM $\mathbb{Z}_m$ UTILIZANDO A REGRA DE CRAMER

**Joseane Alves de Sousa**

Dissertação apresentada ao Departamento de Matemática Pura e Aplicada da Universidade Regional do Cariri como parte dos requisitos exigidos para a obtenção do título de Mestre em matemática.

**Orientador**

Prof. Dr. José Tiago Nogueira Cruz

Juazeiro do Norte - CE

2023

Ficha Catalográfica elaborada pelo autor através do sistema  
de geração automático da Biblioteca Central da Universidade Regional do Cariri - URCA

De Sousa, Joseane Alves

D278r Resolução de Sistemas Lineares em  $Z_m$  utilizando a Regra de Cramer /  
Joseane Alves De Sousa. Juazeiro-CE, 2023.

87p. il.

Dissertação. Mestrado Profissional em Matemática em Rede Nacional da  
Universidade Regional do Cariri - URCA.

Orientador(a): Prof. Dr. José Tiago Nogueira Cruz

1.Sistemas Lineares, 2.Regra de Cramer, 3.Anéis; I.Título.

CDD: 510

# RESOLUÇÃO DE SISTEMAS LINEARES EM $\mathbb{Z}_m$ UTILIZANDO A REGRA DE CRAMER

Joseane Alves de Sousa

Dissertação apresentada ao Departamento de Matemática Pura e Aplicada da Universidade Regional do Cariri como parte dos requisitos exigidos para a obtenção do título de Mestre em matemática.

Aprovada em: 08 / 09 / 2023.

BANCA EXAMINADORA

---

Prof. Dr. José Tiago Nogueira Cruz - Orientador (URCA)

---

Prof. Dr. Alessandro Coelho Alencar (URCA)

---

Prof. Me. Francisco Genilson Dos Santos Silva (SME-Crato)

# Agradecimentos

Agradeço a Deus em primeiro lugar por me capacitar para realização desse curso e desse trabalho científico. Agradeço a minha família em especial a meus filhos David de Sousa Sampaio e Gabriel de Sousa Sampaio, a minha mãe maria de Fátima Alves de Sousa e meus dois irmão Diego Alves de Sousa e Jéssica Alves de Sousa pelo apoio e incentivo nos diversos trabalhos por mim realizados durante esse curso. Aos meus amigos do curso do mestrado profissional em matemática em especial a Antônio Pedro Duarte Moreira e Mardônio Manoel Nogueira de Lima pelas doses de ânimo todas as vezes que me permiti fraquejar durante esse curso. Pelos dias de estudo em grupo para que pudéssemos aprender juntos os conteúdos abordados principalmente no ENQ (exame nacional de qualificação). Aos professores Flavio França Cruz, Pedro Ferreira de Lima (in memória) ,Zelalber Gondim Guimarães, Francisco Valdemiro Braga, Jocel Faustino Norberto de Oliveira, Antônio Ednardo de Oliveira, José Tiago Nogueira Cruz, Francisca Leidmar Josué Viana , que me proporcionaram tanto aprendizado dentro do curso do mestrado e evolução na carreira docente. Ao professor Jocel Faustino Norberto por ter dedicado tempo extra ao currículo escolar para nos proporcionar mais conhecimento para a avaliação do ENQ (Exame de Nacional de Qualificação), tempo esse que resultou na aprovação de muitos de nós estudantes. Ao professor José Tiago Nogueira Cruz pelo apoio e dedicação e ter me dado condições de realizar este trabalho. Enfim agradeço a todos os amigos e familiares que contribuíram de maneira direta ou indireta para que eu pudesse realizar esse sonho agora real de cursar mestrado e então concluí-lo com êxito.

“A imaginação é mais importante que o conhecimento.” (Albert Einstein)

## Resumo

A Regra de Cramer é usada para resolver sistemas de equações lineares. Essencialmente, exigirmos que o sistema tenha o mesmo número de equações e incógnitas. Em seguida, analisamos o determinante da matriz dos coeficientes que é obtida através da representação matricial do sistema. Para encontrar a solução de um sistema linear é necessário exigir que determinante seja não nulo. Caso o determinante seja nulo temos duas situações: o sistema não tem soluções ou possui infinitas soluções. Vamos estender esses conceitos para os anéis  $\mathbb{Z}_m$ .

**Palavras-chave:** Sistemas Lineares, Regra de Cramer, Anéis

## Abstract

Cramer's Rule is used to solve systems of linear equations. Essentially, we require that the system has the same number of equations and unknowns. Then, we analyze the determinant of the coefficient matrix that is obtained through the matrix representation of the system. To find the solution of a linear system, it is necessary to require that the determinant is non-zero. If the determinant is zero, we have two situations: the system has no solutions or it has infinite solutions. Let's extend these concepts to the rings  $\mathbb{Z}_m$ .

**Keywords:** Linear Systems, Cramer's Rule, Rings.

# Sumário

<b>1</b>	<b>Introdução</b>	<b>13</b>
<b>2</b>	<b>Anéis, Domínios e Corpos</b>	<b>16</b>
<b>3</b>	<b>Anéis <math>\mathbb{Z}_m</math></b>	<b>21</b>
<b>4</b>	<b>Subanéis, Subdomínios e Subcorpos</b>	<b>30</b>
<b>5</b>	<b>A regra de Cramer e o Sistema Linear em <math>\mathbb{Z}_m</math></b>	<b>37</b>
5.1	Equação linear em $\mathbb{Z}_m$ . . . . .	38
5.2	Solução de Equação linear em $\mathbb{Z}_m$ . . . . .	38
5.3	Sistema linear em $\mathbb{Z}_m$ . . . . .	40
5.4	Solução de um sistema linear em $\mathbb{Z}_m$ . . . . .	41
5.5	Sistema linear possível e sistema linear impossível em $\mathbb{Z}_m$ . . . . .	46
5.6	Sistema linear homogêneo em $\mathbb{Z}_m$ . . . . .	46
<b>6</b>	<b>Resolução de sistemas linear no <math>\mathbb{Z}_m</math></b>	<b>50</b>
<b>7</b>	<b>CONCLUSÃO</b>	<b>82</b>

# 1 Introdução

A resolução de sistemas lineares é uma das principais ferramentas da álgebra linear, utilizada em diversos campos da matemática e da ciência. Em particular, a resolução de sistemas lineares no  $\mathbb{Z}_m$ , onde  $\mathbb{Z}_m$  denota o anel dos inteiros módulo  $m$ , sendo um problema comum e relevante para diversas aplicações.

O conjunto matemático  $\mathbb{Z}_m$  é um conjunto de números inteiros modulares, onde  $m$  é um número inteiro positivo. Ele é amplamente aplicado em criptografia, uma vez que as operações matemáticas realizadas nesse conjunto são reversíveis. Isso permite o uso de sistemas lineares para codificar e decodificar mensagens de forma segura. Além disso, no contexto das redes de computadores, são utilizados algoritmos lineares eficientes para a transmissão e recepção de dados.

Outro exemplo de aplicação de sistemas lineares no conjunto  $\mathbb{Z}_m$  é a resolução de problemas de logística em transportes. Nesse caso, as equações lineares representam as restrições relacionadas à capacidade dos veículos, demanda dos clientes e disponibilidade de recursos. Resolvendo o sistema, é possível determinar o plano ótimo de distribuição, minimizando custos e otimizando a eficiência do transporte.

Além disso, os sistemas lineares no  $\mathbb{Z}_m$  têm aplicações na teoria dos números, especialmente na resolução de congruências lineares. Congruências lineares são equações da forma  $ax \equiv b \pmod{m}$ , onde  $a, b$  e  $m$  são números inteiros. Através da resolução de sistemas lineares no  $\mathbb{Z}_m$ , é possível determinar os valores de  $x$  que satisfazem a congruência.

Vale salientar que os sistemas lineares de equações da forma em que estudamos hoje teve seu início em 1678, com Gottfried W. Leibniz (1646 - 1716). KLINE (1927: p.606) afirmou em seu livro, em 1693, que Leibniz usou um conjunto sistêmico de

índices como coeficiente de um sistema de três equações lineares com duas incógnitas,  $x$  e  $y$ . Reescreveu as equações eliminando as incógnitas e resultou em uma regra a qual conhecemos como determinante de um conjunto de equações lineares.

Apenas 60 anos depois uma aplicação mais precisa e abrangente foi proposta por Gabriel Cramer para a Resolução de Sistemas Lineares. O que conhecemos hoje como a regra de Cramer que foi publicada no livro *Introduction à L'analyse des lignes courbes algébriques*.

O presente trabalho vem portanto buscar informações que tratam da resolução de sistemas lineares no  $\mathbb{Z}_m$ , sendo prioritária a resolução através da regra de Cramer. Estaremos em busca de informações que determinem os casos de sistemas lineares no  $\mathbb{Z}_m$  para a regra de Cramer: sistema possível e determinado (SPD), sistema possível e indeterminado (SPI), e sistema impossível (SI).

Traremos no capítulo 1 a definição de Anéis, Domínios e Corpos. Nesse capítulo traremos as propriedades dos Anéis, consequências dos axiomas de Anéis, mostraremos que todo corpo é um domínio de integridade e se este for finito demonstraremos que é um corpo e ainda alguns exemplos de Anéis.

No capítulo 2 traremos informações referentes aos Anéis  $\mathbb{Z}_m$  como a definição e propriedades do conjunto  $\mathbb{Z}_m$ , definição de classes e operações que estas podem realizar dentro do conjunto  $\mathbb{Z}_m$ .

No capítulo 3 definiremos Subanéis, Subdomínios e Subcorpos. Mostraremos quando um Subconjunto é Subanel e traremos alguns exemplos. Demonstraremos as soluções de determinada equação num domínio de integridade. Mostraremos ainda quando teremos um subanel unitário. Definiremos quando um Subanel é Subdomínio e alguns exemplos, quando um corpo é subcorpo de outro corpo.

No capítulo 4 traremos A Regra de Cramer e o Sistema Linear em  $\mathbb{Z}_m$ , nele abor-

daremos a resolução de sistemas lineares no  $\mathbb{Z}_m$  através da Regra de Cramer.

No caso específico da resolução de sistemas lineares no  $\mathbb{Z}_m$ , buscaremos as possibilidades de podermos utilizar a regra de Cramer <sup>1</sup> para encontrar uma solução. A regra de Cramer é uma fórmula que nos permite encontrar a solução para cada variável do sistema linear, usando determinantes. Para isso, devemos calcular o determinante principal da matriz  $A$  e os determinantes obtidos ao substituir cada coluna de  $A$  pelo vetor  $b$ . A resposta do sistema será então os valores obtidos divididos pelo determinante principal.

É importante ressaltar que a regra de Cramer só pode ser aplicada em sistemas lineares completos, ou seja, sistemas em que a matriz  $A$  seja quadrada e não singular, ou seja, seu determinante é diferente de zero. Além disso, ao trabalhar com anéis, devemos ter cuidado com a existência de soluções múltiplas ou soluções inexistentes, uma vez que a não existência de inverso multiplicativo limita o espaço de possíveis soluções.

Já no capítulo 5 : Resolução de sistemas lineares no  $\mathbb{Z}_m$  através da regra de Cramer, traremos as questões que evidenciam as possibilidades de resolução de sistemas lineares em  $\mathbb{Z}_m$ , sendo ela sistemas possíveis e determinados, sistemas possíveis e indeterminados e sistemas impossíveis.

Em resumo, a resolução de sistemas lineares no  $\mathbb{Z}_m$ , onde  $\mathbb{Z}_m$  é o anel dos inteiros módulo  $m$ , é um problema relevante e comum em diversas aplicações. Para resolvê-lo, podemos utilizar a regra de Cramer, que nos permite calcular a solução para cada variável do sistema. No entanto, devemos ter cuidado com a existência de soluções múltiplas ou inexistentes quando trabalhando com anéis.

## 2 Anéis, Domínios e Corpos

Uma estrutura algébrica é uma  $(n + 1)$  - upla ordenada

$$(A, *1, \dots, *n)$$

onde  $A$  é um conjunto não vazio com  $n$  operações  $*_1, \dots, *_n$  em  $A$ .

Um anel é uma estrutura algébrica  $(A, +, \cdot)$ , satisfazendo às seguintes propriedades:

1. A estrutura algébrica  $(A, +)$  satisfaz as seguintes propriedades

(a) Associatividade:  $(a + b) + c = a + (b + c) \forall a, b, c \in A$ ;

(b) Comutatividade:  $a + b = b + a \forall a, b \in A$ ;

(c) Existência do elemento neutro: Existe um elemento  $0_A \in A$  tal que  $a + 0_A = 0_A + a = a \forall a \in A$ ;

(d) Inverso aditivo: Para cada  $a \in A$ , existe um elemento  $(-a) \in A$  tal que  $a + (-a) = (-a) + a = 0_A$ .

2. A estrutura algébrica  $(A, \cdot)$  satisfaz a associatividade do produto:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

para todo  $a, b, c \in A$ ; 3. Distributividade do produto em relação à soma: para todo  $a, b, c \in A$  temos

(a)  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

(b)  $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ .

Quando não houver risco de confusão, vamos escreveremos  $ab$  em lugar de  $a \cdot b$ . A diferença de dois elementos  $a$  e  $b$  do anel  $A$  será denotada por  $a - b := a + (-b)$ .

Seja  $(A, +, \cdot)$ , um anel. Dizemos que  $A$  é

1. Um anel comutativo se a operação  $\bullet$  é comutativa;
2. Um anel com unidade se a operação  $\cdot$  tem um elemento neutro  $1_A \in A$ , isto é,

$$a \cdot 1_A = 1_A \cdot a = a, \forall a \in A;$$

3. Um corpo se for um anel comutativo, com unidade tal que para todo  $a \in A - \{0\}$ , existe  $a^{-1} \in A - \{0\}$ , chamado de inverso multiplicativo, satisfazendo

$$a \cdot a^{-1} = a^{-1} \cdot a = 1_A.$$

4. Um anel de integridade (ou domínio de integridade) se for um anel comutativo, com unidade e sem divisores de zero, isto é, satisfazendo uma das duas condições abaixo (que são equivalentes):

$$\forall a, b \in A, ab = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

$$\forall a, b \in A, a \neq 0 \text{ e } b \neq 0 \Rightarrow ab \neq 0.$$

Seja  $A$  um anel comutativo com unidade. As unidades desse anel, é o conjunto

$$u(A) = \{a \in A \mid \exists b \in A; ab = ba = 1\}.$$

Observação 1. Corpo é qualquer anel comutativo com unidade satisfazendo a igualdade

$$\mathcal{U}(A) = A - \{0_A\}.$$

Exemplo 1. Nem todo domínio é corpo. De fato, note que  $\mathbb{Z}$  é um anel comutativo com unidade e

$$\mathcal{U}(\mathbb{Z}) = \{\pm 1\} \neq \mathbb{Z} - \{0\}.$$

Proposição 1 (Consequências dos axiomas de Anéis). Seja  $(A, +, \cdot)$  um anel. Para todo  $a, b \in A$  temos

i)  $a \cdot 0 = 0 \cdot a = 0.$

ii)  $(-a) \cdot b = a \cdot (-b) = -(ab).$

iii)  $(-a) \cdot (-b) = a \cdot b.$

**Demonstração:** i) De fato,

$$\begin{aligned} a \cdot 0 &= a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \\ &\Rightarrow a \cdot 0 = 0. \end{aligned}$$

ii) Note que

$$(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0$$

Portanto,

$$(-a) \cdot b = -(a \cdot b).$$

iii) Segue do item anterior.

Um domínio de integridade e um corpo serão denotados, salvo o contrário, por  $D$  e  $K$ , respectivamente.

Pelo o que foi visto acima, temos que todo corpo é anel e que todo domínio é anel. Vamos agora estabelecer a relação entre corpo e domínio.

Observação 2. É comum escrever  $ab$  ao invés de  $a \cdot b$ .

Proposição 2. Todo corpo é um domínio de integridade.

Demonstração: Seja  $a, b \in K$  tal que

$$ab = 0.$$

Mostremos que  $a = 0$  ou  $b = 0$ . Vamos supor a contradição, isto é,  $a \neq 0$  e  $b \neq 0$ . Como  $K$  é um corpo,  $a$  tem o inverso multiplicativo  $a^{-1}$ . Assim,

$$\begin{aligned} a^{-1}(ab) &= a^{-1}0 = 0 \\ \Rightarrow b &= 0 \end{aligned}$$

o que é uma contradição, pois  $b \neq 0$ .

Portanto,  $K$  não contém nenhum divisor zero e será um domínio de integridade.

Proposição 3. Todo domínio de integridade finito é um corpo.

Demonstração: Seja  $D$  um domínio de integridade e  $a \in D$  com  $a \neq 0$ . Considere o subconjunto de  $D$

$$\{a, a^2, a^3, \dots\}$$

Pela finitude do domínio de integridade, existem  $m, n \in \mathbb{N}$  com  $m < n$  tal que

$$a^m = a^n.$$

Assim,

$$0 = a^m - a^n = a^m (1 - a^{n-m}).$$

Como  $a^m \neq 0$  temos que

$$1 - a^{n-m} = 0.$$

Portanto,

$$a \cdot a^{n-m-1} = 1,$$

ou seja,  $a^{n-m-1}$  é o inverso multiplicativo de  $a$ .

Exemplo 2. Seja  $n \in \mathbb{Z}$ . O conjunto  $(n \cdot \mathbb{Z}, +, \cdot)$ , onde

$$n \cdot \mathbb{Z} = \{na \mid a \in \mathbb{Z}\},$$

é um anel com as operações usuais de soma e produto de  $\mathbb{Z}$ .

Exemplo 3. Com as operações usuais,  $(\mathbb{Z}, +, \cdot)$  é um domínio de integridade, mas não é um corpo. De fato, a unidade do produto é 1 e se  $a \in \mathbb{Z} - \{1\}$ , não existe  $b \in \mathbb{Z}$  tal que  $ab = 1$ .

Exemplo 4. O conjunto dos números reais  $(\mathbb{R}, +, \cdot)$  munido com as operações usuais de soma e produto é um corpo.

Exemplo 5. O conjunto das matrizes de ordem  $n$  com entradas reais  $M_n(\mathbb{R})$  munido das operações usuais de adição e multiplicação de matrizes é um anel com unidade  $I = Id_n(\mathbb{R})$  igual a matriz identidade de ordem  $n$ . No entanto não é um anel comutativo e possui divisores de zero, isto é, existem elementos  $A$  e  $B$  satisfazendo  $A \neq 0, B \neq 0$  e  $AB = 0$ . Exemplo 7. No conjunto  $\mathbb{Z}$  defina as operações:

$$- a *_1 b = a + b$$

$$- a *_2 b = 0.$$

Como a operação  $*_1$  é a adição usual, os axiomas da soma 1.(a) - (d) são verificados.

Veamos agora os axiomas 2. e 3. dos anéis. Tome  $a, b, c \in \mathbb{Z}$

$$a *_2 (b *_2 c) = 0 = (a *_2 b) *_2 c,$$

$$a *_2 (b *_1 c) = 0 = 0 + 0 = (a *_2 b) + (a *_2 c) = (a *_2 b) *_1 (a *_2 c),$$

$$(a *_1 b) *_2 c = 0 = 0 + 0 = (a *_2 c) + (b *_2 c) = (a *_2 c) *_1 (b *_2 c).$$

Segue que  $(\mathbb{Z}, *_1, *_2)$  é anel.

E mais,  $A$  é um anel comutativo, pois

$$a *_2 b = 0 = b *_2 a,$$

para todo  $a, b \in \mathbb{Z}$ .

Note que  $(\mathbb{Z}, *_1, *_2)$  não tem unidade. Com efeito, suponha que não e seja  $x \in \mathbb{Z}$  sua unidade. Em particular,

$$5 = x *_2 5 = 0,$$

o que é um absurdo. Isso prova também que  $(\mathbb{Z}, *_1, *_2)$  não é domínio. Observe ainda que  $(\mathbb{Z}, *_1, *_2)$  possui divisores de zero, pois  $2 \neq 0, 3 \neq 0$  e  $2 *_2 3 = 0$ .

### 3 Anéis $\mathbb{Z}_m$

O produto cartesiano de dois conjuntos  $A$  e  $B$ , denotado por  $A \times B$ , é

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Uma relação  $\mathcal{R}$  entre o conjunto  $A$  é um subconjunto do produto cartesiano  $A \times A$ , isto é, uma relação em  $A$  é um subconjunto  $\mathcal{R} \subset A \times A$ .

Sejam  $a, b \in A$ . Se  $(a, b) \in \mathcal{R}$  dizemos que  $a$  está relacionado com  $b$  e denotamos  $a \sim$

$b$  ou  $a\mathcal{R}b$ . Quando  $a$  não está com  $b$  denotaremos  $a\overline{\mathcal{R}}b$ . Vamos denotar  $\mathcal{R}$  simplesmente por  $\sim$ .

Dizemos que uma relação  $\sim$  em  $A$  é

1. Reflexiva se  $a \sim a$  para todo  $a \in A$ ;
2. simétrica se  $a \sim b$  implica em  $b \sim a$  para todos  $a, b \in A$ ;
3. transitiva se  $a \sim b$  e  $b \sim c$  implicam em  $a \sim c$  para todos  $a, b, c \in A$ .

Caso  $\sim$  seja reflexiva, simétrica e transitiva, dizemos que  $\sim$  é uma relação de equivalência.

Exemplo 8. Dados  $a, b \in \mathbb{R}$ . Defina a relação

$$a \sim b \iff a - b \in \mathbb{Z}$$

Mostraremos que é uma relação de equivalência. De fato,

1. (reflexiva) Claramente,  $a - a = 0 \in \mathbb{Z}$ ;
2. (simétrica) Se  $a - b = c \in \mathbb{Z}$ , então  $b - a = -c \in \mathbb{Z}$ ;
3. (transitiva) Se  $a - b = k_1 \in \mathbb{Z}$  e  $b - c = k_2 \in \mathbb{Z}$ , então  $a - c = (k_1 + b) - (b - k_2) = k_1 + k_2 \in \mathbb{Z}$ .

Sejam  $a, b \in \mathbb{Z}$ . Dizemos que  $a$  é côngruo a  $b$  módulo  $m$ , e escrevemos

$$a \equiv b \pmod{m},$$

se  $m \mid (a - b)$ , ou seja, se existe  $k \in \mathbb{Z}$  tal que  $mk = a - b$ .

Exemplo 9. A relação de congruência módulo o inteiro  $m$  é uma relação de equivalência denotada por  $\sim_m$ . De fato, fixado  $m \in \mathbb{Z}$ , para todos  $a, b, c \in \mathbb{Z}$ ,

1. Reflexiva: sempre temos  $a \sim a$ .

De fato,  $a \equiv a \pmod{m}$ , pois  $m \mid 0$ .

2. Simétrica: se  $a \sim b$ , então  $b \sim a$ .

Suponha que  $a \equiv b \pmod{m}$ . Note que  $b \equiv a \pmod{m}$ , pois se  $m \mid (a - b)$ , então  $m \mid (b - a)$ .

3. Transitiva: Se  $a \sim b$  e  $b \sim c$ , então  $a \sim c$ .

Suponha que  $m \mid (a - b)$  e  $m \mid (b - c)$ . Dessa maneira,  $m \mid [(a - b) + (b - c)]$ , ou seja,  $m \mid (a - c)$ .

Em um conjunto  $A$  munido de uma relação de equivalência. Definimos a classe de equivalência de um elemento  $a \in A$ , com respeito à relação de congruência, como sendo

$$[a] = \bar{a} = \{b \in A \mid a \sim b\}.$$

Note que a classe de equivalência de um elemento  $a \in A$  nunca é vazia, ou seja,  $[a] \neq \emptyset$  para todo  $a \in A$ . Isto é consequência da reflexividade. Uma outra consequência que vem agora da transitividade das classes de equivalência é

$$\bar{a} = \bar{b} \Leftrightarrow a \sim b$$

Uma partição de um conjunto  $A$  é uma família de conjuntos  $A_1, A_2, \dots, A_n$  tais que

$$\bigcup_{i=1}^n A_i = A$$
$$A_i \cap A_j = \emptyset, \text{ se } i \neq j.$$

Teorema 1. Seja uma relação de equivalência em um conjunto  $A$ . As classes de equivalência definidas por são uma partição de  $A$ . Em outras palavras, temos as afirmações abaixo

1. Se  $\bar{a} \neq \bar{b}$ , então  $\bar{a} \cap \bar{b} = \emptyset$

2.  $\bigcup_{a \in A} \{\bar{a}\} = A$

**Demonstração:**

1. Seja  $c \in \bar{a} \cap \bar{b}$ . Assim,  $a \sim c$  e  $c \sim b$ . Dessa maneira, teríamos  $a \sim b$ , o que é uma contradição. Logo,  $\bar{a} \cap \bar{b} = \emptyset$ .

2. A união de todas as classes de equivalência é o próprio  $A$ . Para ver isso, basta notar que todo elemento de  $A$  pertence a uma classe de equivalência e em todas as classes tem apenas elementos que pertencem a  $A$ .

Quando  $A$  é munido de uma relação de equivalência, podemos definir o quociente de  $A$  por  $\sim$  como sendo o conjunto das classes de equivalência

$$A/\sim := \{\bar{a} \mid a \in A\}$$

Exemplo 10. A aplicação

$$\pi : A \longrightarrow A/\sim$$

$$a \longmapsto \bar{a}$$

define uma relação de equivalência em  $A$  da seguinte maneira: Dados  $a, b \in A$ , então

$$a \sim b \Rightarrow \pi(a) = \pi(b).$$

O conjunto das classe de congruências módulo  $m$  ou inteiros módulo  $m$  é o conjunto quociente

$$\mathbb{Z}/\sim_m = \mathbb{Z}/\equiv \text{ mod } m = \{\bar{a} \mid a \in \mathbb{Z}\},$$

onde  $\bar{a} = \{b \in \mathbb{Z} \mid b \equiv a \text{ mod } m\}$ .

Observação 3. Uma outra maneira de associar a classe  $\bar{a} \in \mathbb{Z}_m$  é

$$\bar{a} = a + m\mathbb{Z}$$

Proposição 4. Fixado  $m \in \mathbb{Z}, m \geq 2$ , temos que  $\bar{0}, \bar{1}, \dots, \overline{m-1}$  é uma partição de  $\mathbb{Z}_m$ , ou seja,

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

e cada classe acima é duas a duas disjuntas.

Demonstração: Dado  $a \in \mathbb{Z}$ , temos que  $a \equiv r \text{ mod } m$ , sendo  $r$  o resto da divisão euclidiana de  $a$  por  $m$ . Lembre-se que,  $0 \leq r \leq m-1$ .

Assim, temos  $\bar{a} = \bar{r}$ . Portanto,

$$\mathbb{Z}_m \subset \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

Provemos agora que as classes  $\bar{0}, \bar{1}, \dots, \overline{m-1}$  são duas a duas distintas. Seja  $r_1, r_2 \in \mathbb{Z}$  satisfazendo  $0 \leq r_1 < r_2 \leq m-1$ . Se  $\bar{r}_2 = \bar{r}_1$  então  $r_1 \equiv r_2 \text{ mod } m$ , ou seja,  $m \mid (r_1 - r_2)$ . Isso não acontece, pois  $r_2 - r_1 < m$ .

Observação 4. Quando  $n = 0$  ou  $n = 1$  temos

$$\mathbb{Z}_0 = \{\dots, -\bar{2}, -\bar{1}, \bar{0}, \bar{1}, \bar{2}, \dots\}$$

$$\mathbb{Z}_1 = \{\bar{0}\},$$

pois

$$\bar{a} = a + 0 \cdot \mathbb{Z} \quad \text{e} \quad \bar{0} = 0 + 1 \cdot \mathbb{Z}.$$

As operações de adição e multiplicação em  $\mathbb{Z}_m$  são definidas por:

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} & \cdot : \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} \\ (\bar{a}, \bar{b}) &\longmapsto \bar{a} + \bar{b} & (\bar{a}, \bar{b}) &\longmapsto \bar{a} \cdot \bar{b} \end{aligned}$$

onde  $\bar{a} + \bar{b} = \overline{a+b}$  e  $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

Teorema 2. As operações de adição e multiplicação em  $\mathbb{Z}_m$  estão bemdefinidas.

Mais precisamente, se  $a, b, a', b' \in \mathbb{Z}$  com  $\bar{a} = \overline{a'eb} = \bar{b}'$ , então

$$\begin{aligned} \frac{a+}{b} &= \frac{a'+}{b'} \\ \frac{a \cdot}{b} &= \frac{a' \cdot}{b'}. \end{aligned}$$

Em resumo, as classes de congruência em  $\mathbb{Z}_m$  que definem  $\bar{a} + \bar{b}$  e  $\bar{a} \cdot \bar{b}$  não dependem dos inteiros  $a$  e  $b$  que representam essas classes.

Demonstração: Sejam  $a, b, a', b' \in \mathbb{Z}$ . Como  $\bar{a} = \overline{a'eb}$  e  $\bar{b} = \bar{b}'$ , ou seja,  $a \equiv a' \pmod{m}$  e  $b \equiv b' \pmod{m}$  temos

$$a + b \equiv (a' + b') \pmod{m}$$

$$a \cdot b \equiv a' \cdot b' \pmod{m}$$

$$\log_0 \pi + b = \pi' + b' e \pi \cdot b = \pi' \cdot b'$$

Proposição 5 . O terno  $(\mathbb{Z}_m, +, \cdot)$  é anel comutativo com unidade.

Demonstração: Sejam  $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ .

1.(a) Comutatividade da soma

$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$$

1.(b) Associatividade da soma

$$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{(b+c)} = \overline{a+(b+c)} = \overline{(a+b)+c} = \overline{(a+b)} + \bar{c} = (\bar{a} + \bar{b}) + \bar{c}$$

1.(c) A classe  $\bar{0}$  é o elemento neutro de  $\mathbb{Z}_m$ , pois  $\bar{a} = \overline{a+0} = \bar{a} + \bar{0}$  e  $\bar{a} = \overline{0+a} = \bar{0} + \bar{a}$ .

1.(d) A classe  $\overline{(-a)}$  é o simétrico de  $\bar{a}$ , pois  $\bar{0} = \overline{(-a)+a} = \overline{(-a)} + \bar{a}$  e  $\bar{0} = \overline{a-a} = \bar{a} + \overline{(-a)}$ .

2. Associatividade do produto

$$\bar{a}(\bar{b}\bar{c}) = \bar{a}(\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = (\bar{a}\bar{b})\bar{c}$$

3. Distributividade da soma com o produto

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a}(\overline{b+c}) = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c}$$

$$(\bar{b} + \bar{c})\bar{a} = (\overline{b+c})\bar{a} = \overline{(b+c)a} = \overline{ba+ca} = \overline{ba} + \overline{ca} = \bar{b}\bar{a} + \bar{c}\bar{a}$$

4. Comutatividade do produto

$$\bar{a}\bar{b} = \bar{b}\bar{a}.$$

5. Unidade

$$\bar{a} = \overline{1 \cdot a} = \bar{1} \cdot \bar{a} \text{ e } \bar{a} = \overline{a \cdot 1} = \bar{a} \cdot \bar{1}$$

Exemplo 11. 1. Tabela de operações em  $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ .

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
·	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$

$\bar{1} \quad \bar{1} \quad \bar{0} \quad \bar{1} \quad \bar{0} \quad \bar{1}$

2. Tabela de operações em  $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ .

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
·	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$

$\bar{1} \quad \bar{1} \quad \bar{2} \quad \bar{0} \quad \bar{1} \quad \bar{0} \quad \bar{1} \quad \bar{2} \quad \bar{2} \quad \bar{2} \quad \bar{0} \quad \bar{1} \quad \bar{2} \quad \bar{0} \quad \bar{2} \quad \bar{1}$

3. Tabela de operações em  $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ .

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$

$\bar{1} \ \bar{1} \ \bar{2} \ \bar{3} \ \bar{0} \ \bar{1} \ \bar{0} \ \bar{1} \ \bar{2} \ \bar{3} \ \bar{2} \ \bar{2} \ \bar{3} \ \bar{0} \ \bar{1} \ \bar{2} \ \bar{0} \ \bar{2} \ \bar{0} \ \bar{2} \ \bar{3} \ \bar{3} \ \bar{0} \ \bar{1} \ \bar{2} \ \bar{3} \ \bar{0} \ \bar{3} \ \bar{2}$

Proposição 6. Seja  $m \in \mathbb{N}$ . O espaço quociente  $\mathbb{Z}_m$  é corpo se, e somente se,  $m$  é primo.

Demonstração: Suponha que  $\mathbb{Z}_m$  é corpo. Seja  $a \in \mathbb{N}$  um divisor de  $m$ . Vamos mostrar que

$$a = 1 \quad \text{ou} \quad a = m.$$

Como  $a \mid m$ , existe  $b \in \mathbb{N}$  tal que  $m = ab$ . Assim,

$$\bar{0} = \bar{m} = \bar{b} = \bar{a} \cdot \bar{b}$$

Em particular, do fato de  $\mathbb{Z}_m$  ser domínio, temos que

$$\bar{a} = \bar{0} \quad \text{ou} \quad \bar{b} = \bar{0}$$

Se  $\bar{a} = \bar{0}$ , então

$$a \equiv 0 \pmod{m} \Rightarrow m \mid a.$$

Como  $m \mid a$  e  $a \mid m$  temos  $a = m$ .

Caso  $\bar{b} = \bar{0}$ , então

$$b \equiv 0 \pmod{m} \Rightarrow mt = b,$$

para algum  $t \in \mathbb{N}$

Substituindo o valor de  $b$  em  $m = ab$  vem que  $m = amt$ . Portanto,  $at = 1$ , conseqüentemente,  $a = 1$ .

Suponha agora que  $m$  é primo. Vamos mostrar agora que todo elemento  $\bar{a} \in \mathbb{Z}_m$  com  $\bar{a} \neq \bar{0}$  tem inverso em  $\mathbb{Z}_m$ . Para isso, primeiramente, note que  $a \in \{1, 2, \dots, m-1\}$ ,  $\text{mdc}(m, a) = 1$ , a identidade de Bezout, garante a existência de  $r, s \in \mathbb{Z}$  tais que  $mr + as = 1$ . Tomando classes módulo  $m$  vem que

$$\bar{1} = \overline{mr + sa} = \overline{mr} + \overline{sa} = \overline{mr} + \overline{as} = \overline{0r} + \overline{as} = \overline{0} + \overline{as} = \overline{as}$$

Portanto,  $\bar{s}$  é o inverso de  $\bar{a}$  e  $\mathbb{Z}_m$  é corpo.

## 4 Subanéis, Subdomínios e Subcorpos

Seja  $(A, +, \cdot)$  um anel e seja  $B \subset A$  um subconjunto não vazio de  $A$ . Dizemos que  $B$  é um subanel de  $A$  se

1. O conjunto  $B$  é fechado nas operações  $+$  e  $\cdot$  de  $A$ , isto é, para todo  $a, b \in B$  temos  $a + b \in B$  e  $a \cdot b \in B$ .
2. A estrutura algébrica  $(B, +, \cdot)$ , onde  $+$  e  $\cdot$  são as restrições das operações de  $A$  ao subconjunto  $B$ , é um anel.

Exemplo 12. Todo anel possui dois subanéis triviais:  $\{0\}$  e  $A$ .

Observação 5. Alguns dos axiomas de anel valem automaticamente nos seus subconjuntos. São elas:

- Comutatividade da adição
- Associatividade da adição
- Associatividade da multiplicação
- Distributividade

Proposição 7. Sejam  $A$  um anel e  $B$  um subconjunto não vazio de  $A$ . Então  $B$  é subanel de  $A$  se, e somente se, para todos  $a, b \in B$  tem-se i)  $a - b \in B$

ii)  $a \cdot b \in B$

Demonstração: Suponha que  $B$  um subanel de  $A$ . Para todo  $a, b \in B$ , temos

$$a - b = a + \underbrace{(-b)}_{\in B} \in B$$

e

$$a \cdot b \in B$$

Reciprocamente, suponha que para todo  $a, b \in B$ , temos

$$a - b \in B$$

e

$$a \cdot b \in B$$

Assim

1.  $0 \in B$ , pois  $b - b \in B$ .
2.  $-b \in B$ , pois  $0 - b \in B$ .
3.  $a + b = a - (-b) \in B$ , pois  $a \in B$  e  $-b \in B$ .

Isto implica que  $B$  é fechado na operação  $+$  do anel  $A$ . Restringindo essas operações ao conjunto  $B$ , a propriedades comutatividade da adição, associatividade da adição,

associatividade da multiplicação e distributivas são herdadas de  $A$ . Resta provar que vale as propriedades: existência do elemento neutro e elemento simétrico.

1.(c) Elemento neutro: Seja  $a \in B$ . Como

$$0_A = a - a \in B$$

é o elemento  $0_A$  é elemento neutro para adição em  $A$ , também será em  $B$ . Portanto,  $0_A = 0_B$ .

1.(d) Inverso aditivo: Seja  $b \in B$ . Como  $0_A \in B$  tem-se  $0_A - b = -b \in B$ . Desde que  $-b$  é o simétrico de  $b$  em  $A$ , segue que  $-b$  é o simétrico de  $b$  em  $B$ .

Observação 6. Seja  $B$  um subanel do anel  $A$ . Se  $A$  é comutativo, é claro que  $B$  é comutativo. Além disso, se  $A$  é um anel sem divisores de zero, então  $B$  também é um anel sem divisores de zero.

Exemplo 13. A unidade de um subanel pode não ser a do anel. Para ver isso, considere o anel  $\mathbb{Z}_{12}$  e defina

$$B = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}.$$

É fácil verificar que  $B$  é um subanel de  $\mathbb{Z}_{12}$ .

Note que  $1_B = \bar{9}$ , pois

$$\bar{9} \cdot \bar{3} = \bar{3}$$

$$\bar{9} \cdot \bar{6} = \bar{6}.$$

$$\bar{9} \cdot \bar{9} = \bar{9}.$$

O subanel  $B$  do Anel  $A$  é chamado de subanel unitário do anel com unidade  $A$  quando  $B$  tem unidade e

$$1_B = 1_A.$$

Exemplo 14. Seja  $n$  um inteiro com  $n > 1$ . O conjunto  $n \cdot \mathbb{Z}$  é subanel de  $\mathbb{Z}$  e não tem unidade.

Exemplo 15. Consideremos o anel  $A = M_2(\mathbb{R})$ . Vamos mostrar que  $B = \{ \text{conjuntos das matrizes antisimétrica} \}$

$$B = \left\{ \left[ \begin{array}{cc} a & b \\ -b & a \end{array} \right] \mid a, b, c \in \mathbb{R} \right\}$$

é um subanel de  $M_2(\mathbb{R})$ . De fato, se

$$X = \left[ \begin{array}{cc} a & b \\ -b & a \end{array} \right] \in B \quad e \quad Y = \left[ \begin{array}{cc} c & d \\ -d & c \end{array} \right] \in B,$$

então

i)

$$X - Y = \left[ \begin{array}{cc} a - c & b - d \\ -(b - d) & a - c \end{array} \right] \in B$$

ii)

$$X \cdot Y = \left[ \begin{array}{cc} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{array} \right] \in B$$

Logo,  $B$  é um subanel do anel  $M_2(\mathbb{R})$ .

Exemplo 16. Com as operações usuais,  $(\mathbb{Z}, +, \cdot)$  é subanel de  $(\mathbb{Q}, +, \cdot)$  e  $(\mathbb{Q}, +, \cdot)$  é subanel de  $(\mathbb{R}, +, \cdot)$ .

Exemplo 17. O conjunto dos números ímpares não é subanel de  $\mathbb{Z}$ , enquanto o conjunto dos números pares é um subanel de  $\mathbb{Z}$ .

Exemplo 18. O conjunto  $\bar{2} \cdot \mathbb{Z}_4 = \{\bar{0}, \bar{2}\}$  é subanel de  $\mathbb{Z}_4$ . Para ver isso, note que

$$\bar{0} \cdot \bar{0} = \bar{2} \cdot \bar{0} = \bar{2} \cdot \bar{2} = \bar{0} \in \bar{2} \cdot \mathbb{Z}_4$$

$$\bar{0} - \bar{0} = \bar{2} - \bar{2} = \bar{0} \in \bar{2} \cdot \mathbb{Z}_4$$

$$\bar{0} - \bar{2} = \bar{2} - \bar{0} = \bar{2} \in \bar{2} \cdot \mathbb{Z}_4$$

Lema 1. Num domínio de integridade  $(A, +, \cdot)$ , as únicas soluções da equação  $x^2 = x$  são 0 e 1.

Demonstração: Note que

$$x^2 - x = x \cdot x - x \cdot 1 = x \cdot (x - 1).$$

Assim,  $x^2 - x = 0$  implica em  $x \cdot (x - 1) = 0$ . Como  $A$  é um domínio de integridade, segue que  $x = 0$  ou  $x - 1 = 0$ .

log  $O$

$$x = 0 \quad \text{ou} \quad x = 1.$$

Proposição 8. Seja  $A$  um domínio e  $B$  um subanel com unidade. Se  $1_A$  é a unidade de  $A$  e  $1_B$  a unidade de  $B$ , então  $1_A = 1_B$ .

Demonstração: Note que  $1_B$  é raiz de  $x^2 = x$  e  $1_B \neq 0$ .

Corolário 1. Um subanel com unidade de um domínio é um subanel unitário.

Seja  $A$  um domínio e  $B$  um subanel de  $A$ . Dizemos que  $B$  é um subdomínio de  $A$  quando

1.  $B$  é subanel unitário de  $A$ ;

2.  $B$  é um domínio.

Corolário 2. Sejam  $A$  um domínio e  $B$  um subanel de  $A$ . Então  $B$  é subdomínio de  $A$  se, e somente se,  $B$  tem unidade.

Demonstração: Se  $B$  é subdomínio de  $A$ , é claro que  $B$  tem unidade, pois em particular  $B$  é domínio. Reciprocamente, suponha que  $B$  é um anel com unidade. O corolário acima garante que  $B$  é unitário e  $1_A = 1_B$ . Como  $B$  é subanel do domínio  $A$  (comutativo e não tem divisores de zero), segue que  $B$  comutativo e não tem divisores de zero. Logo,  $B$  é subdomínio de  $A$ . Exemplo 19. Como  $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}[\sqrt{p}] \subseteq \mathbb{Q}[\sqrt{p}]$  possui unidade, segue que

- $\mathbb{Z}$  é subdomínio de  $\mathbb{Q}$ .
- $\mathbb{Z}$  é subdomínio de  $\mathbb{Z}[\sqrt{p}]$ .
- $\mathbb{Z}[\sqrt{p}]$  é subdomínio de  $\mathbb{Q}[\sqrt{p}]$ .
- $\mathbb{Q}[\sqrt{p}]$  é subdomínio de  $\mathbb{R}$ .
- $\mathbb{Q}$  é subdomínio de  $\mathbb{Q}[\sqrt{p}]$ .
- $\mathbb{Q}$  é subdomínio de  $\mathbb{R}$ .

Seja  $A$  um corpo e  $B$  é um subanel de  $A$ . Dizemos que  $B$  é um subcorpo de  $A$  quando

1.  $B$  é subanel unitário de  $A$ ;
2.  $B$  é um corpo.

Observação 7. Note que se  $A$  é corpo,  $B \subseteq A$  e  $B$  é corpo com as operações de  $A$ , então  $B$  é subcorpo de  $A$ .

Proposição 9. Seja  $A$  um corpo e  $B$  um subanel de  $A$ . Então  $B$  é um subcorpo de  $A$  se, e somente se,  $B$  tem unidade e para todo  $b \in B$  com  $b \neq 0$ , existe  $b^{-1} \in B$ .

Demonstração: Suponha que  $B$  é um subcorpo de  $A$ . Por definição, dado  $b \in B$  com  $b \neq 0$ , existe  $b^{-1} \in B$ . Além disso,  $1_B = 1_A$ . Reciprocamente, suponha que  $B$  tem unidade e que para qualquer  $b \in B$  com  $b \neq 0$ , existe  $b^{-1} \in B$ . Como  $B$  é um subanel de  $A$  e  $A$

é comutativo, segue que  $B$  é comutativo. Além disso, como  $B$  tem unidade e  $A$  é domínio (pois  $A$  é corpo), segue que  $B$  é unitário (e portanto tem unidade). Exemplo 20. O conjunto  $\mathbb{Q}[\sqrt{p}]$ , com  $p$  primo, é um subcorpo de  $\mathbb{R}$ . Defato,

$1 = 1 + 0\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$  é a unidade e se  $x = a + b\sqrt{p} \neq 0$ , seu inverso é

$$x^{-1} = \left( \frac{a}{a^2 - pb^2} \right) - \left( \frac{b}{a^2 - pb^2} \right) \sqrt{p}.$$

Proposição 10. Sejam  $A$  um anel e  $B_1, B_2 \subseteq A$ .

1. Se  $B_1$  e  $B_2$  são subanéis de  $A$ , então  $B_1 \cap B_2$  é subanel de  $A$ .
2. Se  $B_1$  e  $B_2$  são subdomínios de  $A$ , então  $B_1 \cap B_2$  é subdomínio de  $A$ .
3. Se  $B_1$  e  $B_2$  são subcorpos de  $A$ , então  $B_1 \cap B_2$  é subcorpo de  $A$ .

**Demonstração:**

1. Sejam  $a, b \in B_1 \cap B_2$ . Como  $a, b \in B_1$  e  $B_1$  é subanel, segue que  $a - b, ab \in B_1$ . Da mesma forma, temos que  $a - b, ab \in B_2$ . Portanto  $a - b, ab \in B_1 \cap B_2$  e  $B_1 \cap B_2$  é subanel de  $A$ .
2. Supondo que  $B_1$  e  $B_2$  são subdomínios de  $A$ , temos que  $B_1$  e  $B_2$  têm a mesma unidade de  $A$ . Então  $1_A \in B_1 \cap B_2$ . Como  $B_1 \cap B_2$  é um subanel do domínio  $A$ ,

segue que  $B_1 \cap B_2$  é subdomínio de  $A$ .

3. Suponha que  $B_1$  e  $B_2$  são subcorpos de  $A$ . Em particular,  $B_1$  e  $B_2$  são subdomínios de  $A$ , o item anterior garante que  $B_1 \cap B_2$  tem unidade  $1_A$ . Seja agora  $b \in B_1 \cap B_2, b \neq 0$ . Como  $b \in B_1$  e  $B_1$  é corpo, temos que  $b^{-1} \in B_1$ . Analogamente  $b^{-1} \in$

## 5 A regra de Cramer e o Sistema Linear em $\mathbb{Z}_m$

A ideia de determinante como polinômio que associa a um quadrado de números, surgiu em 1683 com o matemático japonês Seki Kowa (1637-1708), porém o mesmo não demonstrou para os casos gerais. Logo depois em 1683, o matemático Leibniz (1649-1716) usou combinações de coeficientes para resolver sistemas de coeficientes para resolver sistemas de equações lineares e organizou em forma de índices os coeficientes com números.

Em 1750, no livro "introdução à análise de curvas algébricas", o suíço Gabriel Cramer (1704 - 1752), apresentou resultados para matrizes de ordem  $n$  sendo uma forma de resolução através de determinante de sistemas de equações lineares. Muir (1890: p 9), a regra de Cramer, como hoje a conhecemos, foi apresentada como um apêndice de sua *Introduction à L'analyse* e visava simplificar o tratamento algébrico necessário para a solução do sistema de  $n$  equações lineares com  $n$  incógnitas (ao qual

---

<sup>01</sup> Cramer. Gabriel Cramer, born at Geneva in 1704, and died at Bagnols in 1752, was professor at Geneva. The work by which he is best known is his treatise on algebraic curves 1 published in 1750, which, as far as it goes, is fairly complete; it contains the earliest demonstration that a curve of the  $n$ th degree is in general determined if  $12n(n + 3)$  points on it be given. This work is still sometimes read. Besides this, he edited the works of the two elder Bernoullis; and wrote on the physical cause of the spheroidal shape of the planets and the motion of their apses, 1730, and on Newton's treatment of cubic curves, 1746.

foi reduzido o problema das cônicas).

Vamos nesse capítulo estudar um pouco de sistemas lineares aplicados a resolução de equações lineares no conjunto  $\mathbb{Z}_m$ . Essa abordagem trará a definição de equações lineares no  $\mathbb{Z}_m$ , solução de equações definida no conjunto  $\mathbb{Z}_m$  e sua abordagem através da regra de Cramer.

## 5.1 Equação linear em $\mathbb{Z}_m$

Chamamos de equação linear em  $\mathbb{Z}_m$ , nas incógnitas  $x_1, x_2, x_3, x_4 \dots x_n$  toda equação do tipo  $\overline{a_{11}}x_1 + \overline{a_{12}}x_2 + \overline{a_{13}}x_3 + \dots + \overline{a_{1n}}x_n = \overline{b}$ .

As classes  $\overline{a_{11}}, \overline{a_{12}}, \overline{a_{13}}, \dots, \overline{a_{1n}} \in \mathbb{Z}_m$ , são chamados coeficientes e  $\overline{b} \in \mathbb{Z}_m$ , é o termo independente da equação.

Exemplos:

a)  $\overline{3}x_1 + \overline{4}x_2 - \overline{5}x_3 - x_4 = \overline{5}$  em  $\mathbb{Z}_7$

b)  $x + y = \overline{1}$  em  $\mathbb{Z}_3$

c)  $\overline{0}x_1 + \overline{0}x_2 - \overline{0}x_3 = \overline{5}$  em  $\mathbb{Z}_{11}$

d)  $\overline{0}x_1 + \overline{0}x_2 - \overline{0}x_3 + \overline{0}x_4 = \overline{0}$  em  $\mathbb{Z}_5$

## 5.2 Solução de Equação linear em $\mathbb{Z}_m$

Dizemos que a sequência de classes  $(\overline{a_{11}}, \overline{a_{12}}, \overline{a_{13}}, \dots, \overline{a_{1n}})$  em  $\mathbb{Z}_m^n$ , é uma solução da equação linear  $\overline{a_{11}}x_1 + \overline{a_{12}}x_2 + \overline{a_{13}}x_3 + \dots + \overline{a_{1n}}x_n = \overline{b}$  em  $\mathbb{Z}_m$  se  $\overline{a_{11}}x_1 + \overline{a_{12}}x_2 + \overline{a_{13}}x_3 + \dots + \overline{a_{1n}}x_n = \overline{b}$  for uma série de classes verdadeira.

Exemplo:

a)  $\overline{5}x + \overline{3} = \overline{2}$  em  $\mathbb{Z}_7$

$$\bar{5}x = \bar{2} - \bar{3}$$

$$\bar{5}x = \bar{2} + \bar{4}$$

$$\bar{5}x = \bar{6}$$

O inverso de  $\bar{5}$  em  $\mathbb{Z}_7$  é  $\bar{3}$ , veja na tabela abaixo:

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$

Portanto

$$\bar{5}x = \bar{6}$$

$$x = \bar{6} \cdot \bar{3}$$

$$x = \bar{18}$$

$$x = \bar{4}$$

Portanto a solução desse sistema linear em  $\mathbb{Z}_7$  é  $\bar{4}$

b)  $x + y = \bar{1}$  em  $\mathbb{Z}_3$

Perceba que se  $x = \bar{0}$  então  $y = \bar{1}$ . Se  $x = \bar{1}$  então  $y = \bar{0}$ ,

se  $x = \bar{2}$  então  $y = \bar{2}$ ,

então as possíveis soluções desse sistema linear em  $\mathbb{Z}_3$  são  $(\bar{0}, \bar{1})$ ,  $(\bar{1}, \bar{0})$  ou  $(\bar{2}, \bar{2})$ .

c)  $\bar{2}x - \bar{5} = \bar{1}$  em  $\mathbb{Z}_6$

$$\bar{2}x = \bar{1} + \bar{5}$$

$$\bar{2}x = \bar{6}$$

$$\bar{2}x = \bar{0}$$

O inverso de  $\bar{2}$  em  $\mathbb{Z}_6$  não existe, veja na tabela abaixo:

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

Mas pela perceba ainda que apesar de não haver seu inverso, podemos encontrar a solução, pois  $\bar{2}x = \bar{0}$  os valores para x podem ser  $\bar{0}$  ou  $\bar{3}$ .

### 5.3 Sistema linear em $\mathbb{Z}_m$

É um conjunto solução de  $n(n > 1)$  equações lineares em  $\mathbb{Z}_m$ , nas incógnitas  $x_1, x_2, x_3, x_4 \dots x_n$ .

Assim o sistema:

$$\left\{ \begin{array}{l} \bar{a}_{11}x_1 + \bar{a}_{12}x_2 + \bar{a}_{13}x_3 + \dots + \bar{a}_{1n}x_n = \bar{b}_1 \\ \bar{a}_{21}x_1 + \bar{a}_{22}x_2 + \bar{a}_{23}x_3 + \dots + \bar{a}_{2n}x_n = \bar{b}_2 \\ \bar{a}_{31}x_1 + \bar{a}_{32}x_2 + \bar{a}_{33}x_3 + \dots + \bar{a}_{3n}x_n = \bar{b}_3 \\ \dots \\ \bar{a}_{n1}x_1 + \bar{a}_{n2}x_2 + \bar{a}_{n3}x_3 + \dots + \bar{a}_{nn}x_n = \bar{b}_n \end{array} \right.$$

É linear em  $\mathbb{Z}_m$ .

Pela definição de produto de matrizes, notemos que o sistema linear  $S$  em  $\mathbb{Z}_m$ . pode ser escrito na forma matricial.

Exemplos:

matricial:

$$\begin{pmatrix} \bar{2} & \bar{1} \\ \bar{6} & \bar{3} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{5} \\ \bar{10} \end{pmatrix}$$

$$\text{b) } \begin{cases} \bar{2}x + y = \bar{3} \\ x - y = \bar{4} \end{cases}, \text{ em } \mathbb{Z}_7, \text{ pode ser escrito na forma matricial:}$$

$$\begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & -\bar{1} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{3} \\ \bar{4} \end{pmatrix}$$

## 5.4 Solução de um sistema linear em $\mathbb{Z}_m$

Dizemos que a sequência de classes  $(\bar{\alpha}_{11}, \bar{\alpha}_{12}, \bar{\alpha}_{13}, \dots, \bar{\alpha}_{1n})$  em  $\mathbb{Z}_m$ , é uma solução do sistema linear  $S$ , se for solução de todas as equações de  $S$ .

$$\begin{cases} \bar{a}_{11}x_1 + \bar{a}_{12}x_2 + \bar{a}_{13}x_3 + \dots + \bar{a}_{1n}x_n = b_1 \\ \bar{a}_{21}x_1 + \bar{a}_{22}x_2 + \bar{a}_{23}x_3 + \dots + \bar{a}_{2n}x_n = b_2 \\ \bar{a}_{31}x_1 + \bar{a}_{32}x_2 + \bar{a}_{33}x_3 + \dots + \bar{a}_{3n}x_n = b_3 \\ \dots \\ \bar{a}_{n1}x_1 + \bar{a}_{n2}x_2 + \bar{a}_{n3}x_3 + \dots + \bar{a}_{nn}x_n = b_n \end{cases}$$

Exemplos:

a) O Sistema linear em  $\mathbb{Z}_5$

$$\begin{cases} \bar{2}x + \bar{2}y = \bar{1} \\ \bar{2}x + y = \bar{2} \end{cases}$$

Vamos isolar o termo  $x$  na segunda equação:

$$\bar{2}x + y = \bar{2}$$

$$y = \bar{2} - \bar{2}x$$

Substituindo na primeira equação temos:

$$\bar{2}x + \bar{2}y = \bar{1}$$

$$\bar{2}x + \bar{2}(\bar{2} - \bar{2}x) = \bar{1}$$

$$\bar{2}x + \bar{4} - \bar{4}x = \bar{1}$$

$$\bar{2}x + x = \bar{1} - \bar{4}$$

$$\bar{3}x = \bar{1} + \bar{1}$$

$$\bar{3}x = \bar{2}$$

Precisamos achar o inverso de  $\bar{3}$  em  $\mathbb{Z}_5$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$

Portanto o inverso de  $\bar{3}$  é  $\bar{2}$ . Portanto continuando a resolução temos que:

$$\bar{3}x = \bar{2}$$

$$x = \bar{2} \cdot \bar{2}$$

$$x = \bar{4}$$

Como  $x$  é  $\bar{4}$  substituindo na segunda equação teremos:

$$\bar{2}x + y = \bar{2}$$

$$y = \bar{2} - \bar{2}x$$

$$y = \bar{2} - \bar{2} \cdot \bar{4}$$

$$y = \bar{2} - \bar{8}$$

$$y = \bar{2} + \bar{2}$$

$$y = \bar{4}$$

Portanto os valores de  $x$  e  $y$  no  $\mathbb{Z}_5$ , respectivamente são  $\bar{4}$  e  $\bar{4}$ . Conferindo que os resultados são verdadeiros:

$$\begin{cases} 2x + \bar{2}y = \bar{1} \\ \bar{2}x + y = \bar{2} \end{cases}$$

$$\bar{2}x + \bar{2}y = \bar{1}$$

$$\bar{2} \cdot \bar{4} + \bar{2} \cdot \bar{4} = \bar{1}$$

$$\bar{8} + \bar{8} = \bar{1}$$

$$\bar{16} = \bar{1}$$

$$\bar{1} = \bar{1} \text{ (sentença verdadeira)}$$

A segunda sentença:

$$\bar{2}x + y = \bar{2}$$

$$\bar{2} \cdot \bar{4} + \bar{4} = \bar{2}$$

$$\bar{8} + \bar{4} = \bar{2}$$

$$\bar{12} = \bar{2}$$

$$\bar{2} = \bar{2} \text{ (sentença verdadeira)}$$

b) O sistema linear em  $\mathbb{Z}_7$

$$\begin{cases} x + y = \bar{4} \\ \bar{5}x + \bar{6}y = \bar{3} \end{cases}$$

Vamos utilizar a primeira equação linear e isolar a incógnita  $x$ :

$$x + y = \bar{4}$$

$$x = \bar{4} - y$$

Agora vamos substituir o valor de  $x$  na segunda equação linear:

$$\bar{5}x + \bar{6}y = \bar{3}$$

$$\bar{5}(\bar{4} - y) + \bar{6}y = \bar{3}$$

$$\bar{20} - \bar{5}y + \bar{6}y = \bar{3}$$

$$\bar{2}y + \bar{6}y = \bar{3} - \bar{20}$$

$$\bar{8}y = \bar{3} + \bar{1}$$

$$y = \bar{4}$$

Encontrado o valor de  $y$ , voltamos a primeira equação linear para descobrir o valor de  $x$  :

$$x = \bar{4} - y$$

$$x = \bar{4} - \bar{4}$$

$$x = \bar{4} + \bar{3}$$

$$x = \bar{7}$$

$$x = \bar{0}$$

Portanto os valores de  $(x, y)$  são  $(\bar{0}, \bar{4})$

Conferindo que esse valor é válido em ambas as equações lineares em  $\mathbb{Z}_7$  :

A primeira equação linear:

$$x + y = \bar{4}$$

$$\bar{0} + \bar{4} = \bar{4}$$

$$\bar{4} = \bar{4} \text{ (sentença verdadeira)}$$

A segunda equação linear:

$$\bar{5}x + \bar{6}y = \bar{3}$$

$$\bar{5} \cdot \bar{0} + \bar{6} \cdot \bar{4} = \bar{3}$$

$$\bar{0} + \bar{24} = \bar{3}$$

$$\bar{3} = \bar{3} \text{ (sentença verdadeira)}$$

c) O sistema no  $\mathbb{Z}_{11}$

$$\begin{cases} \bar{2}x + y = \bar{5} \\ \bar{6}x + \bar{3}y = \bar{10} \end{cases}$$

Vamos utilizar a primeira equação linear e isolar a incógnita  $y$ :

$$\bar{2}x + y = \bar{5}$$

$$y = \bar{5} - \bar{2}x$$

Agora vamos substituir o valor de  $y$  na segunda equação linear:

$$\bar{6}x + \bar{3}y = \bar{10}$$

$$\bar{6}x + \bar{3}(\bar{5} - \bar{2}x) = \bar{10}$$

$$\bar{6}x + \bar{15} - \bar{6}x = \bar{10}$$

$$\bar{6}x + \bar{5}x = \bar{10} - \bar{15}$$

$$\bar{0}x = \bar{10} + \bar{7}$$

$$\bar{0}x = \bar{17}$$

$$\bar{0}x = \bar{6}$$

Nesse caso o sistema é impossível que encontremos uma solução dentro do  $\mathbb{Z}_{11}$ .

## 5.5 Sistema linear possível e sistema linear impossível em $\mathbb{Z}_m$

Se um sistema linear S tiver pelo menos uma solução, diremos que ele é possível ou compatível (é o caso do exemplo a e b do item 4.4.); caso não tenha nenhuma solução, diremos que S é impossível ou incompatível (é o caso do exemplo c do item 4.4.).

## 5.6 Sistema linear homogêneo em $\mathbb{Z}_m$

Chamamos de sistema linear homogêneo todo aquele em que o termo independente de todas as equações em  $\mathbb{Z}_m$  iguais a zero.

$$\text{Exemplos: a) } \begin{cases} x + y = \bar{0} \\ \bar{2}x + y + z = \bar{0} \\ \bar{4}x + \bar{3}y + z = \bar{0} \end{cases} \quad \text{b) } \begin{cases} x + y + z = \bar{0} \\ x - y - z = \bar{0} \\ \bar{2}x - y + z = \bar{0} \end{cases}$$

4.7. Resolução de sistemas lineares em  $\mathbb{Z}_m$  através da regra de Cramer.

Considere o sistema de equações lineares  $Ax = b$  em  $\mathbb{Z}_m$ , suponha que A seja uma matriz invertível ( $\det A \neq 0$ ) de ordem n,  $\bar{x} = (\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4 \dots, \bar{x}_n)$  e  $b = (\bar{b}_1, \bar{b}_2, \bar{b}_3, \bar{b}_4 \dots, \bar{b}_n)$  elementos do  $\mathbb{Z}_m^n$ . A regra de Cramer nesta situação, afirma que:

$$x_1 = \frac{\det \begin{pmatrix} \bar{b}_1 & \bar{a}_{12} & \dots & \bar{a}_{1n} \\ \bar{b}_2 & \bar{a}_{22} & \dots & \bar{a}_{2n} \\ \vdots & \vdots & & \vdots \\ \bar{b}_n & \bar{a}_{n2} & \dots & \bar{a}_{nn} \end{pmatrix}}{\det \begin{pmatrix} \bar{a}_{11} & \bar{a}_{12} & \dots & \bar{a}_{1n} \\ \bar{a}_{21} & \bar{a}_{22} & \dots & \bar{a}_{2n} \\ \vdots & \vdots & & \vdots \\ \bar{a}_{n1} & \bar{a}_{n2} & \dots & \bar{a}_{nn} \end{pmatrix}} \quad x_2 = \frac{\det \begin{pmatrix} \bar{a}_{11} & \bar{b}_1 & \dots & \bar{a}_{1n} \\ \bar{a}_{21} & \bar{b}_2 & \dots & \bar{a}_{2n} \\ \vdots & \vdots & & \vdots \\ \bar{a}_{n1} & \bar{b}_n & \dots & \bar{a}_{nn} \end{pmatrix}}{\det \begin{pmatrix} \bar{a}_{11} & \bar{a}_{12} & \dots & \bar{a}_{1n} \\ \bar{a}_{21} & \bar{a}_{22} & \dots & \bar{a}_{2n} \\ \vdots & \vdots & & \vdots \\ \bar{a}_{n1} & \bar{a}_{n2} & \dots & \bar{a}_{nn} \end{pmatrix}},$$

$$x_n = \frac{\det \begin{pmatrix} \overline{a_{11}} & \overline{a_{12}} & \dots & \overline{b_1} \\ \overline{a_{21}} & \overline{a_{22}} & \dots & \overline{b_2} \\ \vdots & \vdots & & \vdots \\ \overline{a_{n1}} & \overline{a_{n2}} & \dots & \overline{b_n} \end{pmatrix}}{\det \begin{pmatrix} \overline{a_{11}} & \overline{a_{12}} & \dots & \overline{a_{1n}} \\ \overline{a_{21}} & \overline{a_{22}} & \dots & \overline{a_{2n}} \\ \vdots & \vdots & & \vdots \\ \overline{a_{n1}} & \overline{a_{n2}} & \dots & \overline{a_{nn}} \end{pmatrix}}$$

Agora considere as matrizes:

$$X_1 = \begin{pmatrix} \overline{x_1} & 0 & \dots & 0 \\ \overline{x_2} & 1 & \dots & 0 \\ \vdots & & & \\ \overline{x_n} & 0 & \dots & 1 \end{pmatrix} = [\overline{x}, e_2, \dots, e_n],$$

$$X_2 = \begin{pmatrix} 1 & \overline{x_1} & \dots & 0 \\ 0 & \overline{x_2} & \dots & 0 \\ \vdots & & & \\ 0 & \overline{x_n} & \dots & 1 \end{pmatrix} = [e_1, \overline{x}, \dots, e_n],$$

...

$$X_n = \begin{pmatrix} 1 & 0 & \dots & \overline{x_1} \\ 0 & 1 & \dots & \overline{x_2} \\ \vdots & & & \vdots \\ 0 & 0 & \dots & \overline{x_n} \end{pmatrix} = [e_1, e_2, \dots, \overline{x}],$$

Note que:

$$A \cdot e_2 = \begin{pmatrix} \overline{a_{11}} & \overline{a_{12}} \cdots & \overline{a_{1n}} \\ \overline{a_{21}} & \overline{a_{22}} \cdots & \overline{a_{2n}} \\ \vdots & \vdots & \vdots \\ \overline{a_{n1}} & \overline{a_{n2}} \cdots & \overline{a_{nn}} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \overline{a_{12}} \\ \overline{a_{22}} \\ \vdots \\ \overline{a_{n2}} \end{pmatrix} = \overline{a_2},$$

Portanto temos:

$$\begin{aligned} A \cdot X_1 &= \begin{pmatrix} \overline{a_{11}} & \overline{a_{12}} \cdots & \overline{a_{1n}} \\ \overline{a_{21}} & \overline{a_{22}} \cdots & \overline{a_{2n}} \\ \vdots & \vdots & \vdots \\ \overline{a_{n1}} & \overline{a_{n2}} \cdots & \overline{a_{nn}} \end{pmatrix} \cdot \begin{pmatrix} \overline{x_1} & 0 \cdots & 0 \\ \overline{x_2} & 1 \cdots & 0 \\ \vdots & \cdots & \\ \overline{x_n} & 0 & \cdots & 1 \end{pmatrix} \\ &= \begin{pmatrix} \overline{a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n} & \overline{a_{12}} \cdots & \overline{a_{1n}} \\ \overline{a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n} & \overline{a_{22}} \cdots & \overline{a_{2n}} \\ \overline{a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n} & \overline{a_{n2}} \cdots & \overline{a_{nn}} \end{pmatrix} \\ &= \begin{bmatrix} Ax, & a_2, \dots, a_n \end{bmatrix} = \begin{bmatrix} b, & a_2, \dots, a_n \end{bmatrix} := M_1 \end{aligned}$$

$$\begin{aligned} A \cdot X_2 &= \begin{pmatrix} \overline{a_{11}} & \overline{a_{12}} \cdots & \overline{a_{1n}} \\ \overline{a_{21}} & \overline{a_{22}} \cdots & \overline{a_{2n}} \\ \vdots & \vdots & \vdots \\ \overline{a_{n1}} & \overline{a_{n2}} \cdots & \overline{a_{nn}} \end{pmatrix} \cdot \begin{pmatrix} 1 & \overline{x_1} \cdots & 0 \\ 0 & \overline{x_2} \cdots & 0 \\ \vdots & \overline{x_n} \cdots & 1 \end{pmatrix} \\ &= \begin{pmatrix} \overline{a_{11}} & \overline{a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n} \cdots & \overline{a_{1n}} \\ \overline{a_{21}} & \overline{a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n} & \overline{a_{2n}} \\ \vdots & \vdots & \vdots \\ \overline{a_{n1}} & \overline{a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n} \cdots & \overline{a_{nn}} \end{pmatrix} \\ &= [a_1, Ax, \dots, a_n] = [a_1, b, \dots, a_n] := M_2 \end{aligned}$$

$$\begin{aligned}
A \cdot X_n &= \begin{pmatrix} \overline{a_{11}} & \overline{a_{12}} \dots & \overline{a_{1n}} \\ \overline{a_{21}} & \overline{a_{22}} \dots & \overline{a_{2n}} \\ \vdots & \vdots & \vdots \\ \overline{a_{n1}} & \overline{a_{n2}} \dots & \overline{a_{nn}} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \dots & \overline{x_1} \\ 0 & 1 \dots & \overline{x_2} \\ 0 & 0 \dots & \overline{x_n} \end{pmatrix} \\
&= \begin{pmatrix} \overline{a_{11}} & \overline{a_{12}} \dots & \overline{a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n} \\ \overline{a_{21}} & \overline{a_{22}} \dots & \overline{a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n} \\ \vdots & \vdots & \vdots \\ \overline{a_{n1}} & \overline{a_{n2}} \dots & \overline{a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n} \end{pmatrix} \\
&= \left[ a_1, a_2, \dots, Ax \right] = [a_1, a_2, \dots, b] := M_n
\end{aligned}$$

Portanto temos que:  $\det M_1 = \det A \cdot \det X_1$

$$\det X_1 = \frac{\det M_1}{\det A}, \det M_2 = \det A \cdot \det X_2$$

$$\det X_2 = \frac{\det M_2}{\det A},$$

$$\det M_n = \det A \cdot \det X_n$$

$$\det X_n = \frac{\det M_n}{\det A}$$

observação: como no conjunto  $\mathbb{Z}_m$  não admite a divisão de classes então esta será substituída pela multiplicação com o inverso do determinante de  $A$ , veja:

$$\det M_n = \det A \cdot \det X_n$$

$$\det X_n = \frac{\det M_n}{\det A}$$

$$\det X_n = \det M_n \cdot (\det A)^{-1}$$

Para o sistema de equações lineares em  $\mathbb{Z}_m$ , temos:

a) Quando o determinante de  $A$  possuir inverso em  $\mathbb{Z}_m$ , teremos um sistema possível de solução, sendo esta única ou seja é sistema possível e determinado (SPD).

b) Quando o determinante de  $A$  não possuir inverso em  $\mathbb{Z}_m$ , mas existir solução para os  $\det X_n$  em  $\det M_n = \det A \cdot \det X_n$  teremos um sistema possível e com várias

soluções, ou seja um sistema possível e indeterminado (SPI)

c) Quando o determinante de A não possuir inverso em  $\mathbb{Z}_m$ , e ainda ao menos um dos  $\det X_n$  em  $\det M_n = \det A \cdot \det X_n$  não existir teremos um sistema impossível (SI).

## 6 Resolução de sistemas linear no $\mathbb{Z}_m$

Os exemplos abaixo evidenciarão as três possibilidades de resolução dos sistemas lineares no  $\mathbb{Z}_m$ . São elas sistema possível e determinado (SPD), sistema possível e indeterminado (SPI) e sistema impossível (SI).

EXEMPLO 1 : RESOLVA O SISTEMA EM  $\mathbb{Z}_7$

$$\begin{cases} x + y = \bar{4} \\ \bar{5}x + \bar{6}y = \bar{3} \end{cases}$$

TEMOS QUE

$$\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{5} & \bar{6} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{4} \\ \bar{3} \end{pmatrix}$$

Vamos encontrar os de terminantes:

$$\det \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{5} & \bar{6} \end{pmatrix} = \bar{6} - \bar{5} = \bar{6} + \bar{2} = \bar{8} = \bar{1}$$

$$\det \begin{pmatrix} \bar{4} & \bar{1} \\ \bar{3} & \bar{6} \end{pmatrix} = \bar{24} - \bar{3} = \bar{3} + \bar{4} = \bar{7} = \bar{0}$$

$$\det \begin{pmatrix} \bar{1} & \bar{4} \\ \bar{5} & \bar{3} \end{pmatrix} = \bar{3} - \bar{20} = \bar{3} + \bar{1} = \bar{4}$$

determinando o inverso de  $\bar{1}$  no  $\mathbb{Z}_7$

$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

Portanto o inverso de  $\bar{1}$  é ele próprio.

Agora vamos determinar o valor de  $x$  e  $y$ .

$$X = \frac{\det \begin{pmatrix} \bar{11} & \bar{1} \\ \bar{115} & \bar{20} \end{pmatrix}}{\det \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{5} & \bar{20} \end{pmatrix}} = \frac{\bar{0}}{\bar{1}} = \bar{0} \cdot \bar{1} = \bar{0}$$

$$y = \frac{\det \begin{pmatrix} \bar{1} & \bar{11} \\ \bar{5} & \bar{115} \end{pmatrix}}{\det \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{5} & \bar{20} \end{pmatrix}} = \frac{\bar{4}}{\bar{1}} = \bar{4} \cdot \bar{1} = \bar{4}$$

A solução possível é  $(\bar{0}, \bar{4})$

EXEMPLO 2: RESOLVA O SISTEMA NO  $\mathbb{Z}_{12}$

$$\begin{cases} x + y = \bar{1} \\ 4x + 2y = \bar{2} \end{cases}$$

TEMOS QUE

$$\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{4} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{1} \\ \bar{2} \end{pmatrix}$$

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{4} & \bar{2} \end{pmatrix} = \bar{2} - \bar{4} = \bar{2} + \bar{8} = \bar{10}$$

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{2} & \bar{2} \end{pmatrix} = \bar{2} - \bar{2} = \bar{2} + \bar{10} = \bar{12} = \bar{0}$$

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{4} & \bar{2} \end{pmatrix} = \bar{2} - \bar{4} = \bar{2} + \bar{8} = \bar{10}$$

Agora encontraremos o inverso de  $\bar{10}$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	8	$\bar{9}$	$\bar{10}$	$\bar{11}$
$\bar{10}$	$\bar{0}$	$\bar{10}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{10}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$

Nesse caso como o  $\bar{10}$  não possui inverso no  $\mathbb{Z}_{12}$ .

Para determinar os valores de  $x$  e  $y$  temos que avaliar através da regra de Cramer os possíveis valores por eles assumidos. Temos então que:

$$\det M = \det A \cdot x \quad \text{e} \quad \det N = \det A \cdot y$$

Os valores assumidos em  $x$  são:

$$\bar{10} \cdot x = \bar{0}$$

Portanto  $x$  só poderá ser  $\bar{0}$  ou  $\bar{6}$

Os valores assumidos em  $y$  são:

$$\bar{10} \cdot y = \bar{6}$$

Portanto  $y$  só poderá ser  $\bar{1}$  ou  $\bar{7}$

Perceba que há possibilidades para as incógnitas  $x$  e  $y$  tornando assim o sistema possível e indeterminado (SPI), pois apresenta mais de uma solução.

Fazendo as devidas substituições no Sistema linear em  $\mathbb{Z}_{12}$  temos que os pares ordenados para  $(x, y)$  são:  $(\bar{0}, \bar{1})$  e  $(\bar{6}, \bar{7})$

EXEMPLO 3 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_8$

$$\begin{cases} \bar{2}x - y + z = \bar{3} \\ \bar{3}x + \bar{2}y - z = \bar{1} \\ \bar{5}x - y = \bar{7} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{2} & \bar{-1} & \bar{1} \\ \bar{3} & \bar{2} & \bar{-1} \\ \bar{5} & -1 & \bar{0} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{3} \\ \bar{1} \\ \bar{7} \end{pmatrix}$$

Encontrando os determinantes :

$$\det \begin{pmatrix} \bar{2} & \bar{-1} & \bar{1} \\ \bar{3} & \bar{2} & \bar{-1} \\ \bar{5} & \bar{-1} & \bar{0} \end{pmatrix} = \bar{0} + \bar{5} - \bar{3} - \bar{2} - \bar{10} = \bar{5} + \bar{5} + \bar{6} + \bar{6} = \bar{22} = \bar{6}$$

$$\det \begin{pmatrix} \bar{3} & \bar{-1} & \bar{1} \\ \bar{1} & \bar{2} & \bar{-1} \\ \bar{7} & \frac{1}{\bar{-1}} & \bar{0} \end{pmatrix} = \bar{7} - \bar{1} - \bar{3} - \bar{14} = \bar{7} + \bar{7} + \bar{5} + \bar{2} = \bar{21} = \bar{5}$$

$$\det \begin{pmatrix} \bar{2} & \bar{3} & \bar{1} \\ \bar{3} & \bar{1} & \bar{-1} \\ \bar{5} & \bar{7} & \bar{0} \end{pmatrix} = \bar{7} + \bar{14} + \bar{5} = \bar{26} = \bar{2}$$

$$\det \begin{pmatrix} \bar{2} & \bar{-1} & \bar{3} \\ \bar{3} & \bar{2} & \bar{1} \\ \bar{5} & \bar{-1} & \bar{7} \end{pmatrix} = \bar{28} - \bar{5} - \bar{9} + \bar{21} + \bar{2} - \bar{30} \\ = \bar{4} + \bar{3} + \bar{7} + \bar{5} + \bar{2} + \bar{2} = \bar{23} = \bar{7}$$

encontrando o inverso de  $\bar{6}$  em  $\mathbb{Z}_8$

$$\begin{array}{c|cccccccc} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} & \bar{7} \\ \hline \bar{6} & \bar{0} & \bar{6} & \bar{4} & \bar{2} & \bar{0} & \bar{6} & \bar{4} & \bar{2} \end{array}$$

Perceba que não existe inverso de  $\bar{6}$  em  $\mathbb{Z}_8$ , portanto analisando a regra de Cramer para os valores acima citados temos que:

$$\det M = \det A \cdot x$$

$$\bar{6} \cdot x = \bar{5}$$

Portando não podemos determinar os valores possíveis para  $x$  em  $Z_8$ ,

$$\det N = \det A \cdot y$$

$$\bar{6} \cdot y = \bar{2}$$

Portando os valores possíveis para  $y$  são  $\bar{3}$  ou  $\bar{7}$ ,

$$\det P = \det A \cdot z$$

$$\bar{3} \cdot z = \bar{3}$$

Portando não podemos determinar os valores possíveis para  $z$  em  $Z_8$ , Como não sabemos os valores para  $x$  e  $z$  temos então uma indeterminação desse Sistema linear em  $Z_8$ , tornando o sistema impossível (SI).

EXEMPLO 4: RESOLVA O SISTEMA LINEAR EM  $Z_7$

$$\begin{cases} x + y = \bar{6} \\ x - y = \bar{4} \end{cases}$$

TEMOS QUE

$$\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{6} \\ \bar{4} \end{pmatrix}$$

Encontrando os valores dos determinantes:

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & -1 \end{pmatrix} = \bar{1} - \bar{1} = \bar{6} + \bar{6} = \bar{12} = \bar{5}$$

$$\text{Det} \begin{pmatrix} \bar{6} & \bar{1} \\ -1 & \end{pmatrix} = \bar{6} - \bar{4} = \bar{1} + \bar{3} = \bar{4}$$

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{6} \\ \bar{1} & \bar{4} \end{pmatrix} = \bar{4} - \bar{6} = \bar{4} + \bar{1} = \bar{5}$$

Determinando o inverso de  $\bar{5}$  no  $Z_7$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$

Portanto o inverso de  $\bar{5}$  é  $\bar{3}$  e isso já nos mostra que o sistema é possível e determinado (SPD).

Agora vamos determinar o valor de  $x$  e  $y$ .

$$X = \frac{\text{Det} \begin{pmatrix} \bar{20} & \bar{1} \\ \bar{4} & \frac{-1}{\bar{1}} \end{pmatrix}}{\text{Det} \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & -\bar{1} \end{pmatrix}} = \bar{5} = \bar{4} \cdot \bar{3} = \bar{12} = \bar{5} \quad y = \frac{\text{Det} \begin{pmatrix} \bar{1} & \bar{4} \\ \bar{20} & \bar{4} \end{pmatrix}}{\text{Det} \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & -\bar{1} \end{pmatrix}} = \frac{\bar{5}}{\bar{3}} = \bar{5} \cdot \bar{3} = \bar{15} = \bar{1}$$

Portanto o valor de  $x$  e  $y$  são respectivamente  $\bar{5}$  e  $\bar{1}$

EXEMPLO 5 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_9$

$$\begin{cases} \bar{X} + \bar{Y} = \bar{0} \\ \bar{2X} + \bar{Y} + \bar{Z} = \bar{0} \\ \bar{4X} + \bar{3Y} + \bar{Z} = \bar{0} \end{cases}$$

TEMOS QUE :

$$\begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{2} & \bar{1} & \bar{1} \\ \bar{4} & \bar{3} & \bar{1} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{0} \end{pmatrix}$$

Por Cramer temos:

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{2} & \bar{1} & \bar{1} \\ \bar{4} & \bar{3} & \bar{1} \end{pmatrix} = \bar{1} + \bar{4} + \bar{0} - \bar{2} - \bar{3} - \bar{0} = \bar{5} + \bar{7} + \bar{6} = \bar{18} = \bar{0}$$

$$\text{Det} \begin{pmatrix} \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{0} & \bar{3} & \bar{1} \end{pmatrix} = \bar{0}$$

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{2} & \bar{0} & \bar{1} \\ \bar{4} & \bar{0} & \bar{1} \end{pmatrix} = \bar{0}$$

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{2} & \bar{1} & \bar{0} \\ \bar{4} & \bar{3} & \bar{0} \end{pmatrix} = \bar{0}$$

Como os determinante acima são zero temos que o sistema não apresentará inverso para o determinante A. Analisando pela regra de Cramer temos que:

$$\text{det } M = \text{det } A \cdot x$$

$$\bar{0} \cdot x = \bar{0}$$

Portando os valores possíveis para x são  $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}$   $\text{det } N = \text{det } A \cdot y$

$$\bar{0} \cdot y = \bar{0}$$

Portando os valores possíveis para y são  $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}$

$$\text{det } P = \text{det } A \cdot z$$

$$\bar{0} \cdot z = \bar{0}$$

Portando os valores possíveis para z são  $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}$

O Sistema linear apresenta mais de uma solução para as incógnitas x, y, z, tornando assim o sistema possível e indeterminado (SPI). Duas soluções possíveis são  $(\bar{0}, \bar{0}, \bar{0})$  e  $(\bar{8}, \bar{1}, \bar{1})$ .

EXEMPLO 6 : RESOLVA O SISTEMA EM  $\mathbb{Z}_5$

$$\begin{cases} 2x - y = \bar{2} \\ -x + \bar{3}y = \bar{-3} \end{cases}$$

TEMOS QUE

$$\begin{pmatrix} \bar{2} & -\bar{1} \\ -1 & \bar{3} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{2} \\ \bar{-3} \end{pmatrix}$$

$$\text{Det} \begin{pmatrix} \bar{2} & -\bar{1} \\ -1 & \bar{3} \end{pmatrix} = \bar{6} - \bar{1} = \bar{6} + \bar{4} = \bar{10} = \bar{0}$$

$$\text{Det} \begin{pmatrix} \bar{2} & -\bar{1} \\ -\bar{3} & \bar{3} \end{pmatrix} = \bar{6} - \bar{3} = \bar{6} + \bar{2} = \bar{8} = \bar{3} \quad \text{Det} \begin{pmatrix} \bar{2} & \bar{2} \\ -\bar{1} & -\bar{3} \end{pmatrix} = -\bar{6} + \bar{2} = \bar{4} + \bar{2} = \bar{6} = \bar{1}$$

Nesse caso como o  $\bar{0}$  não possui inverso no  $\mathbb{Z}_5$  então vamos analisar os possíveis valores de  $xy$ .

Para determinar os valores de  $x$  e  $y$  temos que avaliar através da regra de Cramer os possíveis valores por eles assumidos. Temos então que:

$$\det M = \det A \cdot x \quad \text{e} \quad \det N = \det A \cdot y$$

Os valores assumidos em  $x$  são:

$$\bar{0} \cdot x = \bar{3}$$

Portanto  $x$  não assumira valores no  $\mathbb{Z}_5$

Os valores assumidos em  $y$  são:

$$\bar{0} \cdot y = \bar{1}$$

Portanto  $y$  não admitirá valores no  $\mathbb{Z}_5$

Temos então que os valores para  $x$  e  $y$  neste sistema não são possíveis, com isso o sistema é impossível (SI).

EXEMPLO 7: RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_{11}$

$$\begin{cases} \bar{2}x + \bar{3}y = \bar{7} \\ \bar{5}x + y = \bar{6} \end{cases}$$

TEMOS QUE

$$\begin{pmatrix} \bar{2} & \bar{3} \\ \bar{5} & \bar{1} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{7} \\ \bar{6} \end{pmatrix}$$

$$\det \begin{pmatrix} \bar{2} & \bar{3} \\ \bar{5} & \bar{1} \end{pmatrix} = \bar{2} - \bar{15} = \bar{2} + \bar{7} = \bar{9}$$

$$\det \begin{pmatrix} \bar{7} & \bar{3} \\ \bar{6} & \bar{1} \end{pmatrix} = \bar{7} - \bar{18} = \bar{7} + \bar{4} = \bar{11} = \bar{0}$$

$$\det \begin{pmatrix} \bar{2} & \bar{7} \\ \bar{5} & \bar{6} \end{pmatrix} = \bar{12} - \bar{35} = \bar{1} + \bar{9} = \bar{10}$$

Agora precisamos saber quem é o inverso de  $\bar{9}$  no  $\mathbb{Z}_{11}$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$
$\bar{11}$	$\bar{0}$	$\bar{9}$	$\bar{7}$	$\bar{10}$	$\bar{3}$	$\bar{1}$	$\bar{10}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$

Determinamos que o inverso de  $\bar{9}$  no  $\mathbb{Z}_{11}$  é  $\bar{5}$ , portanto o sistema é possível e determinado (SPD), em seguida iremos determinar os valores para  $x$  e  $y$ .

$$y = \frac{\det \begin{pmatrix} 2 & \frac{7}{5} \\ \frac{2}{5} & \frac{3}{3} \end{pmatrix}}{\frac{1}{10}} = \frac{\bar{10}}{\bar{9}} = \bar{10} \cdot \bar{5} = \bar{50} = \bar{6}$$

Portanto o valor de  $x$  e  $y$  são respectivamente  $\bar{0}$  e  $\bar{6}$ .

EXEMPLO 8: RESOLVA O SISTEMA EM  $\mathbb{Z}_5$

$$\begin{cases} \bar{2}x + \bar{3}y = \bar{4} \\ x - y = \bar{2} \end{cases}$$

TEMOS QUE

$$\begin{pmatrix} \bar{2} & \bar{3} \\ \bar{1} & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{4} \\ \bar{2} \end{pmatrix}$$

$$\text{Det} \begin{pmatrix} \bar{2} & \bar{3} \\ \bar{1} & -1 \end{pmatrix} = \bar{-2} - \bar{3} = \bar{3} + \bar{2} = \bar{5} = \bar{0}$$

$$\text{Det} \begin{pmatrix} \bar{4} & \bar{3} \\ \bar{1} & -1 \end{pmatrix} = \bar{-4} - \bar{6} = \bar{1} + \bar{4} = \bar{5} = \bar{0}$$

$$\text{Det} \begin{pmatrix} \bar{2} & \bar{4} \\ \bar{1} & \bar{2} \end{pmatrix} = \bar{4} - \bar{4} = \bar{2} + \bar{1} = \bar{5} = \bar{0}$$

Nesse caso como o  $\bar{0}$  não possui inverso no  $\mathbb{Z}_5$ .

Para determinar os valores de x e y temos que avaliar através da regra de Cramer os possíveis valores por eles assumidos. Temos então que:

$$\det M = \det A \cdot \det x \quad \text{e} \quad \det M = \det A \cdot \det y$$

Os valores assumidos em x são:

$$\bar{0} \cdot x = \bar{0}$$

Portanto x poderá ser  $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$

Os valores assumidos em y são:

$$\bar{0} \cdot y = \bar{0}$$

Portanto y poderá ser  $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$

Portanto temos valores assumidos para as incógnitas x e y, sendo assim o sistema é possível e indeterminado (SPI).

Fazendo as devidas substituições no Sistema linear em  $\mathbb{Z}_{12}$  temos que os pares ordenados para (x, y) são:  $(\bar{1}, \bar{4}), (\bar{2}, \bar{0}), (\bar{3}, \bar{1}), (\bar{4}, \bar{2}), (\bar{0}, \bar{3})$

EXEMPLO 9 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_6$

$$\begin{cases} \bar{2}x + \bar{3}y - z = \bar{0} \\ x - \bar{2}y + z = \bar{5} \\ -x + y + z = \overline{-2} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{2} & \bar{3} & \overline{-1} \\ \bar{1} & \overline{-2} & \bar{1} \\ \overline{-1} & \bar{1} & \bar{1} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{0} \\ \bar{5} \\ \overline{-2} \end{pmatrix}$$

Encontrando os determinantes :

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{2} & \bar{3} & \overline{-1} \\ \bar{1} & \overline{-2} & \bar{1} \\ \overline{-1} & \bar{1} & \bar{1} \end{pmatrix} &= \overline{-2} - \bar{3} - \bar{1} - \bar{3} - \bar{2} + \bar{2} \\ &= \bar{4} + \bar{3} + \bar{5} + \bar{3} + \bar{4} + \bar{2} = \overline{21} = \bar{3} \end{aligned}$$

$$\begin{aligned} \det \begin{pmatrix} \bar{0} & \bar{3} & \overline{-1} \\ \bar{5} & \overline{-2} & \bar{1} \\ \overline{-2} & \bar{1} & \bar{1} \end{pmatrix} &= \bar{0} - \bar{6} - \bar{5} - \overline{15} - \bar{0} + \bar{4} \\ &= \bar{1} + \bar{3} + \bar{4} = \bar{8} = \bar{2} \end{aligned}$$

\$\$

$\operatorname{det}$  left(

$$\begin{pmatrix} \bar{2} & \bar{0} & \overline{-1} \\ \bar{1} & \frac{\bar{5}}{\overline{-1}} & \bar{1} \\ \overline{-2} & \bar{1} & \end{pmatrix}$$

right)= $\overline{10} + \overline{2} + \overline{4} + \overline{5} = \overline{21} = \overline{3}$

$$\det \begin{pmatrix} \bar{2} & \bar{3} & \bar{0} \\ \bar{1} & \bar{-2} & \bar{5} \\ \bar{-1} & \bar{-2} & \bar{-2} \end{pmatrix} = \bar{8} - \bar{15} + \bar{6} + \bar{10} = \bar{8} + \bar{3} + \bar{6} + \bar{10} = \bar{27} = \bar{3}$$

encontrando o inverso de  $\bar{3}$  no  $\mathbb{Z}_6$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$0$	$3$	$\bar{0}$	$\bar{3}$

Perceba que não existe inverso de  $\bar{3}$  em  $\mathbb{Z}_6$ , portanto analisando a regra de Cramer para os valores acima citados temos que:

$$\det M = \det A \cdot x$$

$$\bar{3} \cdot x = \bar{2}$$

Portando não podemos determinar os valores possíveis para  $x$  em  $\mathbb{Z}_6$ ,

$$\det N = \det A \cdot y$$

$$\bar{3} \cdot y = \bar{3}$$

Portando os valores possíveis para  $y$  são  $\bar{1}, \bar{3}$  ou  $\bar{5}$ ,

$$\det P = \det A \cdot z$$

$$\bar{3} \cdot z = \bar{3}$$

Portando os valores possíveis para  $z$  são  $\bar{1}, \bar{3}$  ou  $\bar{5}$ ,

Como não sabemos os valores para  $x$  temos então uma indeterminação desse Sistema linear em  $\mathbb{Z}_6$ .

EXEMPLO 10 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_{11}$

$$\begin{cases} x - \bar{2}y - \bar{2}z = \bar{-1} \\ x - y + z = \bar{-2} \\ \bar{2}x + y + \bar{3}z = \bar{1} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{1} & \bar{-2} & \bar{-2} \\ \bar{1} & \bar{-1} & \bar{1} \\ \bar{2} & \bar{1} & \bar{3} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{-1} \\ \bar{-2} \\ \bar{1} \end{pmatrix}$$

Encontrando os determinantes:

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{1} & \bar{-2} & \bar{-2} \\ \bar{1} & \bar{-1} & \bar{1} \\ \bar{2} & \bar{1} & \bar{3} \end{pmatrix} &= \bar{-3} - \bar{4} - \bar{2} + \bar{6} - \bar{1} - \bar{4} \\ &= \bar{8} + \bar{7} + \bar{9} + \bar{6} + \bar{10} + \bar{7} = \bar{47} = \bar{3} \end{aligned}$$

$$\begin{aligned} \det \begin{pmatrix} \bar{-1} & \bar{-2} & \bar{-2} \\ \bar{-2} & \bar{-1} & \bar{1} \\ \bar{1} & \bar{1} & \bar{3} \end{pmatrix} &= \bar{3} - \bar{2} + \bar{4} - \bar{12} + \bar{1} - \bar{2} \\ &= \bar{3} + \bar{9} + \bar{4} + \bar{10} + \bar{1} + \bar{9} = \bar{36} = \bar{3} \end{aligned}$$

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{1} & \bar{-1} & \bar{-2} \\ \bar{1} & \bar{-2} & \bar{1} \\ \bar{2} & \bar{1} & \bar{3} \end{pmatrix} &= \bar{-6} - \bar{2} - \bar{2} + \bar{3} - \bar{1} - \bar{8} \\ &= \bar{5} + \bar{9} + \bar{9} + \bar{3} + \bar{10} + \bar{3} = \bar{39} = \bar{6} \end{aligned}$$

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{1} & \bar{-2} & \bar{-1} \\ \bar{1} & \bar{-1} & \bar{-2} \\ \bar{2} & \bar{1} & \bar{1} \end{pmatrix} &= \bar{-1} + \bar{8} - \bar{1} + \bar{2} + \bar{2} - \bar{2} \\ &= \bar{10} + \bar{8} + \bar{10} + \bar{2} + \bar{2} + \bar{9} = \bar{41} = \bar{8} \end{aligned}$$

encontrando o inverso de  $\bar{3}$  no  $\mathbb{Z}_{11}$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$8$	$\bar{9}$	$\bar{10}$
$\bar{3}$	$\bar{0}$	$3$	$\bar{6}$	$\bar{9}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{10}$	$\bar{2}$	$\bar{5}$	$\bar{8}$

O inverso de  $\bar{3}$  é  $\bar{4}$  em  $\mathbb{Z}_{11}$ , tornando o sistema possível e determinado (SPD)

Agora para encontrar o valor de  $x, y$  e  $z$  temos:

A solução possível é  $(\bar{1}, \bar{2}, \bar{10})$

EXEMPLO 11 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_4$

$$\begin{cases} x + y = \bar{1} \\ -\bar{2}x + \bar{3}y - \bar{3}z = \bar{2} \\ x + z = \bar{1} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ -\bar{2} & \bar{3} & -\bar{3} \\ \bar{1} & \bar{0} & \bar{1} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{1} \\ \bar{2} \\ \bar{1} \end{pmatrix}$$

Encontrando os determinantes :

$$\det \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ -\bar{2} & \bar{3} & \bar{-3} \\ \bar{1} & \bar{0} & \bar{1} \end{pmatrix} = \bar{3} - \bar{3} + \bar{0} - \bar{2} + \bar{0} + \bar{0} = \bar{3} + \bar{1} + \bar{2} = \bar{6} = \bar{2}$$

$$\det \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{2} & \bar{3} & \bar{-3} \\ \bar{1} & \bar{0} & \bar{1} \end{pmatrix} = \bar{3} - \bar{3} + \bar{0} - \bar{2} - \bar{0} - \bar{0} = \bar{3} + \bar{1} + \bar{2} = \bar{6} = \bar{2}$$

$$\det \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ -\bar{2} & \bar{2} & \bar{-3} \\ \bar{1} & \bar{1} & \bar{1} \end{pmatrix} = \bar{2} - \bar{3} + \bar{0} + \bar{2} + \bar{3} + \bar{0} = \bar{2} + \bar{1} + \bar{2} + \bar{3} = \bar{8} = \bar{0}$$

$$\det \begin{pmatrix} \bar{1} & \bar{1} & \bar{1} \\ \bar{-2} & \bar{3} & \bar{2} \\ \bar{1} & \bar{0} & \bar{1} \end{pmatrix} = \bar{3} + \bar{2} + \bar{0} + \bar{2} + \bar{0} - \bar{3} = \bar{3} + \bar{2} + \bar{2} + \bar{1} = \bar{8} = \bar{0}$$

encontrando o inverso de  $\bar{2}$  em  $\mathbb{Z}_4$

$$\frac{\begin{array}{c|cccc} & \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \hline \bar{2} & \bar{0} & \bar{2} & \bar{0} & \bar{2} \end{array}}{\bar{2}}$$

Perceba que não existe inverso de  $\bar{2}$  em  $\mathbb{Z}_4$ , portanto analisando a regra de Cramer para os valores acima citados temos que:

$$\det M = \det A \cdot x$$

$$\bar{2} \cdot x = \bar{2}$$

Portando os valores possíveis para x são  $\bar{1}$  ou  $\bar{3}$ ,

$$\det N = \det A \cdot y$$

$$\bar{2} \cdot y = \bar{0}$$

Portando os valores possíveis para y são  $\bar{0}$  ou  $\bar{2}$ ,  $\det P = \det A \cdot Z$

$$2.z = \bar{0}$$

Portando os valores possíveis para  $z$  são  $\bar{0}$  ou  $\bar{2}$ ,

Sabendo os possíveis valores para  $x, y$  e  $z$ , temos que o sistema linear é possível e indeterminado (SPI), pois apresenta mais de uma solução. Através da substituição encontramos as possíveis soluções são  $(\bar{1}, \bar{0}, \bar{0})$  e  $(\bar{3}, \bar{2}, \bar{2})$ .

EXEMPLO 12 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_7$

$$\begin{cases} x + y - z = \bar{0} \\ x - y - \bar{2}z = \bar{1} \\ x - \bar{2}y + z = \bar{4} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{1} & \bar{1} & \overline{-1} \\ \bar{1} & \overline{-1} & \overline{-2} \\ \bar{1} & \overline{-2} & \bar{1} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{0} \\ \bar{1} \\ \bar{4} \end{pmatrix}$$

Encontrando os determinantes:

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{1} & \bar{1} & \overline{-1} \\ \bar{1} & \overline{-1} & \overline{-2} \\ \bar{1} & \overline{-2} & \bar{1} \end{pmatrix} &= \overline{-1} - \bar{2} + \bar{2} - \bar{1} - \bar{4} - \bar{1} \\ &= \bar{6} + \bar{5} + \bar{2} + \bar{6} + \bar{3} + \bar{6} = \overline{28} = \bar{0} \end{aligned}$$

$$\begin{aligned} \det \begin{pmatrix} \bar{0} & \bar{1} & \overline{-1} \\ \bar{4} & \overline{-1} & \overline{-2} \\ \bar{4} & \overline{-2} & \bar{1} \end{pmatrix} &= \bar{0} - \bar{8} + \bar{2} - \bar{1} + \bar{0} - \bar{4} \\ &= \bar{6} + \bar{2} + \bar{6} + \bar{3} = \overline{17} = \bar{3} \end{aligned}$$

$$\det \begin{pmatrix} \bar{1} & \bar{0} & \overline{-1} \\ \bar{1} & \bar{1} & \overline{-2} \\ \bar{1} & \bar{4} & \bar{1} \end{pmatrix} = \bar{1} - \bar{4} + \bar{8} + \bar{1} = \bar{1} + \bar{3} + \bar{8} + \bar{1} = \overline{13} = \bar{6}$$

$$\det \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{1} & \bar{-2} & \bar{1} \end{pmatrix} = \bar{4} + \bar{1} + \bar{0} - \bar{4} + \bar{2} + \bar{0} \\ = \bar{4} + \bar{1} + \bar{3} + \bar{2} = \bar{10} = \bar{3}$$

Perceba que não existe inverso de  $\bar{0}$  em  $\mathbb{Z}_7$ , portanto analisando a regra de Cramer para os valores acima citados temos que:

$$\det M = \det A \cdot x$$

$$\bar{0} \cdot x = \bar{3}$$

Portando não podemos determinar os valores possíveis para x em  $\mathbb{Z}_7$ ,

$$\det N = \det A \cdot y$$

$$\bar{0} \cdot y = \bar{2}$$

Portando não podemos determinar os valores possíveis para y em  $\mathbb{Z}_7$ ,

$$\det P = \det A \cdot z$$

$$\bar{0} \cdot z = \bar{3}$$

Portando não podemos determinar os valores possíveis para z em  $\mathbb{Z}_7$

Como não sabemos os valores para x, y e z temos então uma indeterminação desse Sistema linear em  $\mathbb{Z}_7$ .

EXEMPLO 13 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_5$

$$\begin{cases} \bar{2}x + \bar{3}y = \bar{4} \\ x + \bar{5}y = \bar{2} \end{cases}$$

TEMOS QUE

$$\begin{pmatrix} \bar{2} & \bar{3} \\ \bar{1} & \bar{5} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{4} \\ \bar{2} \end{pmatrix}$$

$$\det \begin{pmatrix} \bar{2} & \bar{3} \\ \bar{1} & \bar{5} \end{pmatrix} = \bar{10} - \bar{3} = \bar{0} + \bar{2} = \bar{2}$$

$$\det \begin{pmatrix} \bar{4} & \bar{3} \\ \bar{2} & \bar{5} \end{pmatrix} = \bar{20} - \bar{6} = \bar{0} + \bar{4} = \bar{4}$$

$$\det \begin{pmatrix} \bar{2} & \bar{4} \\ \bar{1} & \bar{2} \end{pmatrix} = \bar{4} - \bar{4} = \bar{4} + \bar{1} = \bar{5} = \bar{0}$$

determinando o inverso de  $\bar{2}$  no  $\mathbb{Z}_5$

$$\begin{array}{c|ccccc} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \hline \bar{2} & \bar{0} & \bar{2} & \bar{4} & \bar{1} & \bar{3} \end{array}$$

Determinamos que o inverso de  $\bar{2}$  no  $\mathbb{Z}_5$  é  $\bar{3}$ . em seguida iremos determinar os valores para x e y.

$$y = \frac{\det \begin{pmatrix} \bar{2} & \bar{4} \\ \bar{1} & \bar{2} \end{pmatrix}}{\det \begin{pmatrix} \bar{2} & \bar{3} \\ \bar{1} & \bar{5} \end{pmatrix}} = \frac{\bar{0}}{\bar{2}} = \bar{0} = \bar{0} \cdot \bar{3} = \bar{0}$$

Portanto o valor de x e y são respectivamente  $\bar{2}$  e  $\bar{0}$ .

EXEMPLO 14 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_6$

$$\begin{cases} \bar{2}x + y + z = \bar{4} \\ x + \bar{2}y + \bar{2}z = \bar{2} \\ x - y - z = \bar{2} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{2} & \bar{1} & \bar{1} \\ \bar{1} & \bar{2} & \bar{2} \\ \bar{1} & \frac{\bar{2}}{-1} & \frac{-1}{-1} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{4} \\ \bar{2} \\ \bar{2} \end{pmatrix}$$

Encontrando os determinantes:

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{2} & \bar{1} & \bar{1} \\ \bar{1} & \frac{\bar{2}}{\bar{1}} & \frac{\bar{2}}{-1} \end{pmatrix} &= \bar{-4} + \bar{2} - \bar{1} + \bar{1} + \bar{4} - \bar{2} \\ &= \bar{2} + \bar{2} + \bar{5} + \bar{1} + \bar{4} + \bar{4} = \bar{18} = \bar{0} \end{aligned}$$

$$\begin{aligned} \text{det} \begin{pmatrix} \bar{4} & \bar{1} & \bar{1} \\ \bar{2} & \frac{\bar{2}}{\bar{2}} & \frac{\bar{2}}{-1} \end{pmatrix} &= \bar{-8} + \bar{4} - \bar{2} + \bar{2} + \bar{8} - \bar{4} \\ &= \bar{4} + \bar{4} + \bar{4} + \bar{2} + \bar{2} + \bar{2} = \bar{18} = \bar{0} \end{aligned}$$

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{2} & \bar{4} & \bar{1} \\ \bar{1} & \bar{2} & \bar{2} \\ \bar{1} & \bar{2} & \frac{-1}{-1} \end{pmatrix} &= \bar{-4} + \bar{8} + \bar{2} + \bar{4} - \bar{8} - \bar{2} \\ &= \bar{2} + \bar{8} + \bar{2} + \bar{4} + \bar{4} + \bar{4} = \bar{24} = \bar{0} \end{aligned}$$

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{2} & \bar{1} & \bar{4} \\ \bar{1} & \frac{\bar{2}}{\bar{1}} & \bar{2} \\ \bar{1} & \bar{-1} & \bar{2} \end{pmatrix} &= \bar{8} + \bar{2} - \bar{4} - \bar{2} + \bar{4} - \bar{8} \\ &= \bar{8} + \bar{2} + \bar{2} + \bar{4} + \bar{4} + \bar{4} = \bar{24} = \bar{0} \end{aligned}$$

Como os determinantes acima são zero temos de pela regra de Cramer os possíveis valores para x, y e z :

$$\det M = \det A \cdot x$$

$$\bar{0} \cdot x = \bar{0}$$

Portando os valores possíveis para  $x$  são  $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$  det  $N = \det A \cdot y$

$$\bar{0} \cdot y = \bar{0}$$

Portando os valores possíveis para  $y$  são  $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$

$$\det P = \det A \cdot z$$

$$\bar{0} \cdot z = \bar{0}$$

Portando os valores possíveis para  $z$  são  $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$

O Sistema linear apresenta mais de uma solução, tornando-o possível e indeterminado (SPI). São soluções possíveis para esse sistema:  $(\bar{2}, \bar{0}, \bar{0}), (\bar{0}, \bar{4}, \bar{0}), (\bar{0}, \bar{1}, \bar{0}), (\bar{2}, \bar{3}, \bar{3}), (\bar{4}, \bar{1}, \bar{1}), (\bar{4}, \bar{5}, \bar{3}), (\bar{4}, \bar{3}, \bar{5})$ .

EXEMPLO 15 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_{12}$

$$\begin{cases} \bar{2}x - y + z = \bar{-3} \\ \bar{3}x + \bar{2}y - z = \bar{11} \\ \bar{-2}x - \bar{4}y + 3z = \bar{8} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{2} & \bar{-1} & \bar{1} \\ \bar{3} & \bar{2} & \bar{-1} \\ \bar{-2} & \bar{-4} & \bar{3} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{-3} \\ \bar{11} \\ \bar{8} \end{pmatrix}$$

Encontrando os determinantes :

$$\text{Det} \begin{pmatrix} \bar{2} & \bar{-1} & \bar{1} \\ \bar{3} & \bar{2} & \bar{-1} \\ \bar{-2} & \bar{-4} & \bar{3} \end{pmatrix} = \bar{12} - \bar{2} - \bar{12} + \bar{9} - \bar{8} + \bar{4}$$

$$= \bar{0} + \bar{10} + \bar{0} + \bar{9} + \bar{4} + \bar{4} = \bar{27} = \bar{3}$$

$$\det \begin{pmatrix} \bar{-3} & \bar{-1} & \bar{1} \\ \bar{11} & \bar{2} & \bar{-1} \\ \bar{8} & \bar{-4} & \bar{3} \end{pmatrix} = \bar{-18} + \bar{8} - \bar{44} + \bar{33} + \bar{12} - \bar{16}$$

$$= \bar{6} + \bar{8} + \bar{4} + \bar{9} + \bar{0} + \bar{8} = \bar{35} = \bar{11}$$

$$\text{Det} \begin{pmatrix} \bar{2} & \bar{-3} & \bar{1} \\ \bar{3} & \bar{11} & \bar{-1} \\ \bar{-2} & \bar{8} & \bar{3} \end{pmatrix} = \bar{66} - \bar{6} + \bar{24} + \bar{27} + \bar{16} + \bar{22}$$

$$= \bar{6} + \bar{6} + \bar{3} + \bar{4} + \bar{10} = \bar{29} = \bar{5}$$

$$\text{Det} \begin{pmatrix} \bar{2} & \bar{-1} & \bar{-3} \\ \bar{3} & \bar{2} & \bar{11} \\ \bar{-2} & \bar{\frac{-4}{8}} & \bar{8} \end{pmatrix} = \bar{32} + \bar{22} + \bar{36} + \bar{24} + \bar{88} - \bar{12}$$

$$= \bar{8} + \bar{10} + \bar{0} + \bar{0} + \bar{4} + \bar{0} = \bar{22} = \bar{10}$$

encontrando o inverso de  $\bar{3}$  em  $\mathbb{Z}_{12}$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$	$\bar{11}$
$\bar{3}$	$\bar{0}$	$\bar{5}$	$\bar{6}$	$\bar{9}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$

Perceba que não existe inverso de  $\bar{3}$  em  $\mathbb{Z}_{12}$ , portanto analisando a regra de Cramer para os valores acima citados temos que:

$$\det M = \det A \cdot x$$

$$\bar{3} \cdot x = \bar{11}$$

Portando não podemos determinar os valores possíveis para x em  $\mathbb{Z}_{12}$ ,

$$\det N = \det A \cdot y$$

$$\bar{3} \cdot y = \bar{5}$$

Portando não podemos determinar os valores possíveis para y em  $\mathbb{Z}_{12}$ ,

$$\det P = \det A \cdot z \quad \bar{3} \cdot z = \bar{10}$$

Portando não podemos determinar os valores possíveis para z em  $\mathbb{Z}_{12}$ ,

Como não sabemos os valores para x, y e z temos então uma indeterminação desse Sistema linear em  $\mathbb{Z}_{12}$

EXEMPLO 16 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_7$

$$\begin{cases} x + y + z = \bar{6} \\ x - y - z = \bar{-4} \\ \bar{2}x - y + z = \bar{1} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{1} & \bar{1} & \bar{1} \\ \bar{1} & \bar{-1} & \bar{-1} \\ \bar{2} & \bar{-1} & \bar{1} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{6} \\ \bar{-4} \\ \bar{1} \end{pmatrix}$$

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{1} & \bar{1} \\ \bar{1} & \bar{-1} & \bar{-1} \\ \bar{2} & \bar{1} & \bar{1} \end{pmatrix} = \bar{-1} - \bar{2} - \bar{1} - \bar{1} - \bar{1} + \bar{2}$$

$$= \bar{6} + \bar{5} + \bar{6} + \bar{6} + \bar{6} + \bar{2} = \bar{31} = \bar{3}$$

$$\text{Det} \begin{pmatrix} \bar{6} & \bar{1} & \bar{1} \\ \bar{-4} & \bar{-1} & \bar{-1} \\ \bar{1} & \bar{-1} & \bar{1} \end{pmatrix} = \bar{-6} - \bar{1} + \bar{4} + \bar{4} - \bar{6} + \bar{1}$$

$$= \bar{1} + \bar{6} + \bar{4} + \bar{4} + \bar{1} + \bar{1} = \bar{17} = \bar{3}$$

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{6} & \bar{1} \\ \bar{1} & \bar{-4} & \bar{-1} \\ \bar{2} & \bar{1} & \bar{1} \end{pmatrix} = \bar{-4} - \bar{12} + \bar{1} - \bar{6} + \bar{1} + \bar{8}$$

$$= \bar{3} + \bar{2} + \bar{1} + \bar{1} + \bar{1} + \bar{8} = \bar{16} = \bar{2}$$

$$= \bar{6} + \bar{6} + \bar{1} + \bar{6} + \bar{3} + \bar{12} = \bar{34} = \bar{6}$$

encontrando o inverso de  $\bar{3}$  no  $\mathbb{Z}_7$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{3}$	$\bar{0}$	$3$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$

O inverso de  $\bar{3}$  é  $\bar{5}$ .

Agora para encontrar o valor de x, y e z temos:

$$y = \frac{\text{Det} \begin{pmatrix} \frac{1}{1} & \bar{6} & \frac{1}{-1} \\ \frac{1}{2} & \bar{1} & \frac{1}{1} \end{pmatrix}}{\text{Det} \begin{pmatrix} \frac{1}{1} & \bar{1} & \frac{1}{-1} \\ \frac{1}{2} & \frac{1}{-1} & \frac{1}{1} \end{pmatrix}} = \frac{\bar{2}}{\bar{3}} = \bar{2} \cdot \bar{5} = \bar{10} = \bar{3}$$

A solução possível é  $(\bar{1}, \bar{3}, \bar{2})$  EXEMPLO 17: RESOLVA O SISTEMA EM  $\mathbb{Z}_7$

$$\begin{cases} \bar{2}x + y = \bar{3} \\ x - y = \bar{4} \end{cases}$$

TEMOS QUE

$$\begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{3} \\ \bar{4} \end{pmatrix}$$

$$\text{Det} \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & -1 \end{pmatrix} = \bar{-2} - \bar{1} = \bar{5} + \bar{6} = \bar{11} = \bar{4}$$

$$\text{Det} \begin{pmatrix} \bar{3} & \bar{1} \\ \bar{4} & -1 \end{pmatrix} = \bar{-3} - \bar{4} = \bar{4} + \bar{3} = \bar{7} = \bar{0}$$

$$\text{Det} \begin{pmatrix} \bar{2} & \bar{3} \\ \bar{1} & \bar{4} \end{pmatrix} = \bar{8} - \bar{3} = \bar{1} + \bar{4} = \bar{5}$$

Encontrando o inverso de  $\bar{4}$  no  $\mathbb{Z}_7$

$$\begin{array}{c|cccccc} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \hline \bar{4} & \bar{0} & \bar{4} & \bar{1} & \bar{5} & \bar{2} & \bar{6} & \bar{3} \end{array}$$

O inverso de  $\bar{4}$  é  $\bar{2}$ .

Agora para encontrar o valor de x e y temos:

$$X = \frac{\text{Det} \begin{pmatrix} \bar{3} & \bar{1} \\ \bar{4} & \bar{-1} \end{pmatrix}}{\text{Det} \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{1} & \bar{-1} \end{pmatrix}} = \frac{\bar{0}}{\bar{4}} = \bar{0} \cdot \bar{2} = \bar{0}$$

$$y = \frac{\text{Det} \begin{pmatrix} \bar{2} & \bar{3} \\ \bar{1} & \bar{4} \end{pmatrix}}{\text{Det} \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{1} & \bar{-1} \end{pmatrix}} = \frac{\bar{5}}{\bar{4}} = \bar{5} \cdot \bar{2} = \bar{10} = \bar{3}$$

A solução possível é  $(\bar{0}, \bar{3})$

EXEMPLO 18 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_5$

$$\begin{cases} x + y + z = \bar{1} \\ -x - y + z = \bar{1} \\ \bar{2}x + \bar{3}y + \bar{2}z = \bar{0} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{1} & \bar{1} & \bar{1} \\ \bar{-1} & \bar{-1} & \bar{1} \\ \bar{2} & \bar{3} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{1} \\ \bar{1} \\ \bar{0} \end{pmatrix}$$

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{1} & \bar{1} & \bar{1} \\ \bar{-1} & \bar{-1} & \bar{1} \\ \bar{2} & \bar{3} & \bar{1} \end{pmatrix} &= \bar{-2} + \bar{2} - \bar{3} + \bar{2} - \bar{3} + \bar{2} \\ &= \bar{3} + \bar{2} + \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{13} = \bar{3} \end{aligned}$$

$$\text{Det} \begin{pmatrix} \bar{1} & \bar{1} & \bar{1} \\ \bar{1} & \bar{-1} & \bar{1} \\ \bar{0} & \bar{3} & \bar{2} \end{pmatrix} = \bar{-2} + \bar{0} + \bar{3} - \bar{2} - \bar{3} - \bar{0} = \bar{3} + \bar{3} + \bar{3} + \bar{2} = \bar{11} = \bar{1}$$

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{1} & \bar{1} & \bar{1} \\ -\bar{1} & \bar{1} & \bar{1} \\ \bar{2} & \bar{0} & \bar{2} \end{pmatrix} &= \bar{2} + \bar{2} + \bar{0} + \bar{2} - \bar{0} - \bar{2} \\ &= \bar{2} + \bar{2} + \bar{2} + \bar{3} = \bar{9} = \bar{4} \end{aligned}$$

$$\begin{aligned} \text{Det} \begin{pmatrix} \bar{1} & \bar{1} & \bar{1} \\ -\bar{1} & -\bar{1} & \bar{1} \\ \bar{2} & \bar{3} & \bar{0} \end{pmatrix} &= \bar{0} + \bar{2} - \bar{3} + \bar{0} - \bar{3} + \bar{2} \\ &= \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{8} = \bar{3} \end{aligned}$$

encontrando o inverso de  $\bar{3}$  em  $\mathbb{Z}_5$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$

O inverso de  $\bar{3}$  em  $\mathbb{Z}_5$  é  $\bar{2}$ .

Agora para encontrar o valor de x, y e z temos:

$$X = \frac{\text{Det} \begin{pmatrix} \frac{1}{\bar{1}} & \bar{1} & \frac{1}{-\bar{1}} \\ \bar{0} & \bar{3} & \frac{1}{\bar{2}} \end{pmatrix}}{\text{Det} \begin{pmatrix} \bar{1} & \bar{1} & \bar{1} \\ -\bar{1} & -\bar{1} & \frac{1}{\bar{2}} \end{pmatrix}} = \frac{\bar{1}}{\bar{3}} = \bar{1} \cdot \bar{2} = \bar{2}$$

A solução possível é  $(\bar{2}, \bar{3}, \bar{1})$  EXEMPLO 19 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_7$

$$\begin{cases} -x + y - z = \bar{5} \\ x + \bar{2}y + \bar{4}z = \bar{4} \\ \bar{3}x + y - \bar{2}z = \bar{-3} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{-1} & \bar{1} & \bar{-1} \\ \bar{1} & \bar{2} & \bar{4} \\ \bar{3} & \bar{1} & \bar{-2} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{5} \\ \bar{4} \\ \bar{-3} \end{pmatrix}$$

Encontrando os determinantes:

$$\text{Det} \begin{pmatrix} \bar{-1} & \bar{1} & \bar{-1} \\ \bar{1} & \bar{2} & \bar{4} \\ \bar{3} & \bar{1} & \bar{-2} \end{pmatrix} = \bar{4} + \bar{12} - \bar{1} + \bar{2} + \bar{4} + \bar{6}$$

$$= \bar{4} + \bar{12} + \bar{6} + \bar{2} + \bar{4} + \bar{6} = \bar{34} = \bar{6}$$

$$\text{det} \begin{pmatrix} \bar{5} & \bar{1} & \bar{-1} \\ \bar{4} & \bar{2} & \bar{4} \\ \bar{-3} & \bar{1} & \bar{-2} \end{pmatrix} = \bar{-20} - \bar{12} - \bar{4} + \bar{8} - \bar{20} - \bar{6}$$

$$= \bar{1} + \bar{2} + \bar{3} + \bar{8} + \bar{1} + \bar{1} = \bar{16} = \bar{2}$$

$$\text{Det} \begin{pmatrix} \bar{-1} & \bar{5} & \bar{-1} \\ \bar{1} & \bar{\frac{4}{3}} & \bar{4} \\ \bar{3} & \bar{-2} & \end{pmatrix} = \bar{8} + \bar{60} + \bar{3} + \bar{10} - \bar{12} + \bar{12}$$

$$= \bar{1} + \bar{4} + \bar{3} + \bar{3} + \bar{2} + \bar{5} = \bar{18} = \bar{4}$$

$$\begin{aligned} \text{Det} \begin{pmatrix} \overline{-1} & \overline{1} & \overline{5} \\ \overline{1} & \overline{2} & \overline{4} \\ \overline{3} & \overline{1} & \overline{-3} \end{pmatrix} &= \overline{6} + \overline{12} + \overline{5} + \overline{3} + \overline{4} - \overline{30} \\ &= \overline{6} + \overline{5} + \overline{5} + \overline{3} + \overline{4} + \overline{5} = \overline{28} = \overline{0} \end{aligned}$$

encontrando o inverso de  $\overline{6}$  no  $\mathbb{Z}_7$

$$\overline{6} \begin{vmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} \\ \overline{0} & \overline{6} & \overline{5} & \overline{4} & \overline{3} & \overline{2} & \overline{1} \end{vmatrix}$$

O inverso de  $\overline{6}$  é  $\overline{6}$ .

Agora para encontrar o valor de  $x, y$  e  $z$  temos:

$$\begin{aligned} X &= \frac{\det \begin{pmatrix} \overline{5} & \overline{1} & \overline{-1} \\ \frac{\overline{4}}{\overline{-3}} & \frac{\overline{1}}{\overline{2}} & \frac{\overline{4}}{\overline{-2}} \end{pmatrix}}{\det \begin{pmatrix} \overline{-1} & \overline{1} & \overline{-1} \\ \overline{1} & \frac{\overline{2}}{\overline{2}} & \frac{\overline{4}}{\overline{-2}} \end{pmatrix}} = \frac{\overline{2}}{\overline{6}} = \overline{2} \cdot \overline{6} = \overline{12} = \overline{5} \\ y &= \frac{\det \begin{pmatrix} \overline{-1} & \overline{5} & \overline{-1} \\ \overline{1} & \frac{\overline{4}}{\overline{3}} & \overline{4} \\ \overline{3} & \frac{\overline{-3}}{\overline{-2}} \end{pmatrix}}{\det \begin{pmatrix} \overline{-1} & \overline{1} & \overline{-1} \\ \overline{1} & \frac{\overline{2}}{\overline{2}} & \frac{\overline{4}}{\overline{-2}} \end{pmatrix}} = \frac{\overline{4}}{\overline{6}} = \overline{4} \cdot \overline{6} = \overline{24} = \overline{3} \end{aligned}$$

A solução possível é  $(\overline{5}, \overline{3}, \overline{0})$

EXEMPLO 20 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_7$

$$\begin{cases} -x - \overline{4}y = \overline{0} \\ \overline{3}x + \overline{2}y = \overline{5} \end{cases}$$

TEMOS QUE

$$\begin{pmatrix} \overline{-1} & \overline{-4} \\ \overline{3} & \overline{2} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \overline{0} \\ \overline{5} \end{pmatrix}$$

$$\text{Det} \begin{pmatrix} \overline{-1} & \overline{-4} \\ \overline{3} & \overline{2} \end{pmatrix} = \overline{-2} + \overline{12} = \overline{5} + \overline{12} = \overline{17} = \overline{3} \quad \text{Det} \begin{pmatrix} \overline{0} & \overline{-4} \\ \overline{5} & \overline{2} \end{pmatrix} = \overline{0} + \overline{20} = \overline{20} = \overline{6}$$

$$\text{Det} \begin{pmatrix} \overline{-1} & \overline{0} \\ \overline{3} & \overline{5} \end{pmatrix} = \overline{-5} - \overline{0} = \overline{2}$$

Agora encontraremos o inverso de  $\overline{3}$  em  $\mathbb{Z}_7$

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$

O inverso de  $\overline{3}$  em  $\mathbb{Z}_7$  é  $\overline{5}$ .

Agora para encontrar o valor de  $x, y$  e  $z$  temos:

$$X = \frac{\text{Det} \begin{pmatrix} \overline{0} & \overline{-4} \\ \overline{5} & \overline{2} \end{pmatrix}}{\text{Det} \begin{pmatrix} \overline{-1} & \overline{2} \\ \overline{3} & \overline{5} \end{pmatrix}} = \frac{\overline{6}}{\overline{3}} = \overline{6} \cdot \overline{5} = \overline{30} = \overline{2}$$

A solução possível para  $x$  e  $y$  é  $(\overline{2}, \overline{3})$

EXEMPLO 21 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_8$

$$\begin{cases} \overline{2}x + y - z = \overline{4} \\ \overline{3}x + \overline{2}y - \overline{5}z = \overline{1} \\ -x - y + z = \overline{-3} \end{cases}$$

Temos:

$$\begin{pmatrix} \overline{\frac{2}{-3}} & \overline{1} & \overline{-1} \\ \overline{-1} & \overline{-1} & \overline{1} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \overline{4} \\ \overline{1} \\ \overline{-3} \end{pmatrix} \quad \text{Encontrando os determinantes:}$$

$$\begin{aligned}
\text{Det} \begin{pmatrix} \frac{\bar{2}}{-\bar{3}} & \frac{\bar{1}}{\bar{2}} & \overline{-1} \\ \overline{-1} & \frac{\overline{-5}}{-\bar{1}} & \bar{1} \end{pmatrix} &= \bar{4} + \bar{5} - \bar{3} + \bar{3} - \overline{10} - \bar{2} \\
&= \bar{4} + \bar{5} + \bar{5} + \bar{3} + \bar{6} + \bar{6} = \overline{29} = \bar{5} \\
\text{det} \begin{pmatrix} \bar{4} & \bar{1} & \overline{-1} \\ \bar{1} & \frac{\bar{2}}{-\bar{3}} & \overline{-5} \\ \overline{-1} & \bar{1} & \end{pmatrix} &= \bar{8} + \overline{15} + \bar{1} - \bar{1} - \overline{20} - \bar{6} \\
&= \bar{8} + \overline{15} + \bar{1} + \bar{7} + \bar{4} + \bar{2} = \overline{37} = \bar{5} \\
\text{Det} \begin{pmatrix} \frac{\bar{2}}{-\bar{3}} & \bar{4} & \overline{-1} \\ \frac{\bar{2}}{-\bar{1}} & \frac{\overline{-5}}{-\bar{3}} & \bar{1} \end{pmatrix} &= \bar{2} + \overline{20} - \bar{9} + \overline{12} - \overline{30} - \bar{1} \\
&= \bar{2} + \overline{20} + \bar{7} + \overline{12} + \bar{2} + \bar{7} = \overline{50} = \bar{2} \\
\text{Det} \begin{pmatrix} \frac{\bar{2}}{-\bar{3}} & \frac{\bar{1}}{\bar{2}} & \frac{\bar{4}}{\bar{1}} \\ \frac{\overline{-1}}{-\bar{1}} & \frac{\bar{1}}{-\bar{3}} & \end{pmatrix} &= \overline{-12} - \bar{1} + \overline{12} - \bar{9} + \bar{2} + \bar{8} \\
&= \bar{4} + \bar{7} + \overline{12} + \bar{7} + \bar{2} + \bar{8} = \overline{40} = \bar{0}
\end{aligned}$$

encontrando o inverso de  $\bar{5}$  no  $Z_8$

$$\begin{array}{c|cccccccc}
& \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} & \bar{7} \\
\bar{5} & \bar{0} & \bar{5} & \bar{2} & \bar{7} & \bar{4} & \bar{1} & \bar{6} & \bar{3}
\end{array}$$

O inverso de  $\bar{5}$  é  $\bar{5}$ .

Agora para encontrar o valor de  $x, y$  e  $z$  temos:

$$y = \frac{\det \begin{pmatrix} \bar{2} & \bar{4} & \bar{-1} \\ \bar{-3} & \bar{2} & \bar{-5} \\ \bar{-1} & \bar{-3} & \bar{1} \end{pmatrix}}{\det \begin{pmatrix} \bar{2} & \bar{1} & \bar{-1} \\ \bar{-3} & \bar{-1} & \bar{1} \\ \bar{-1} & \bar{-1} & \bar{1} \end{pmatrix}} = \frac{\bar{2}}{\bar{5}} = \bar{2} \cdot \bar{5} = \bar{10} = \bar{2}$$

$$z = \frac{\det \begin{pmatrix} \bar{2} & \bar{1} & \bar{4} \\ \bar{-3} & \bar{1} & \bar{-3} \\ \bar{-1} & \bar{-1} & \bar{2} \end{pmatrix}}{\det \begin{pmatrix} \bar{2} & \bar{1} & \bar{-1} \\ \bar{-3} & \bar{2} & \bar{-5} \\ \bar{-1} & \bar{-1} & \bar{1} \end{pmatrix}} = \frac{\bar{5}}{\bar{5}} = \bar{0} \cdot \bar{5} = \bar{0}$$

A solução possível é  $(\bar{1}, \bar{2}, \bar{0})$

EXEMPLO 22 : RESOLVA O SISTEMA LINEAR EM  $\mathbb{Z}_9$

$$\begin{cases} \bar{2}x - y + z = \bar{3} \\ \bar{3}x + \bar{2}y - z = \bar{1} \\ \bar{5}x - y = \bar{7} \end{cases}$$

Temos:

$$\begin{pmatrix} \bar{2} & \bar{-1} & \bar{1} \\ \bar{3} & \bar{2} & \bar{-1} \\ \bar{5} & \bar{-1} & \bar{0} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \bar{3} \\ \bar{1} \\ \bar{7} \end{pmatrix}$$

Encontrando os determinantes:

$$\text{Det} \begin{pmatrix} \bar{2} & \bar{-1} & \bar{1} \\ \bar{3} & \bar{2} & \bar{-1} \\ \bar{5} & \bar{-1} & \bar{0} \end{pmatrix} = \bar{0} + \bar{5} - \bar{3} + \bar{0} - \bar{2} - \bar{10}$$

$$= \bar{5} + \bar{6} + \bar{7} + \bar{8} = \bar{26} = \bar{8}$$

$$\det \begin{pmatrix} \bar{3} & \bar{-1} & \bar{1} \\ \bar{1} & \bar{2} & \bar{-1} \\ \bar{7} & \bar{-1} & \bar{0} \end{pmatrix} = \bar{7} - \bar{1} - \bar{3} - \bar{14} = \bar{7} + \bar{8} + \bar{6} + \bar{4} = \bar{25} = \bar{7}$$

$$\det \begin{pmatrix} \bar{2} & \bar{3} & \bar{1} \\ \bar{3} & \bar{1} & \overline{-1} \\ \bar{5} & \bar{7} & \bar{0} \end{pmatrix} = \overline{-15} + \overline{21} + \overline{14} - \bar{5} = \bar{3} + \overline{21} + \overline{14} + \bar{4} = \overline{42} = \bar{6}$$

$$\det \begin{pmatrix} \bar{2} & \overline{-1} & \bar{3} \\ \bar{3} & \bar{2} & \bar{1} \\ \bar{5} & \overline{-1} & \bar{7} \end{pmatrix} = \overline{28} - \bar{5} - \bar{9} + \overline{21} + \bar{2} - \overline{30}$$

$$= \bar{1} + \bar{4} + \bar{0} + \bar{3} + \bar{2} + \bar{6} = \overline{16} = \bar{7}$$

encontrando o inverso de  $\bar{8}$  no  $Z_9$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

O inverso de  $\bar{8}$  é  $\bar{8}$ .

Agora para encontrar o valor de  $x, y$  e  $z$  temos:

$$y = \frac{\det \begin{pmatrix} \frac{\bar{2}}{\bar{3}} & \bar{3} & \frac{\bar{1}}{\bar{3}} \\ \frac{\bar{1}}{\bar{5}} & \frac{\bar{1}}{\bar{7}} & \bar{0} \\ \det \left( \begin{pmatrix} \frac{\bar{2}}{\bar{3}} & \overline{-1} & \frac{\bar{1}}{\overline{-1}} \end{pmatrix} \right) \\ \bar{5} & \frac{\bar{2}}{\overline{-1}} & \bar{0} \end{pmatrix}}{\bar{0}} = \bar{8} = \bar{6} \cdot \bar{8} = \overline{48} = \bar{3}$$

$$z = \frac{\det \begin{pmatrix} \frac{\bar{2}}{\bar{3}} & \overline{-1} & \bar{3} \\ \bar{5} & \frac{\bar{2}}{\overline{-1}} & \frac{\bar{1}}{\bar{7}} \end{pmatrix}}{\det \begin{pmatrix} \bar{2} & \overline{-1} & \bar{1} \\ \frac{\bar{3}}{\bar{5}} & \frac{\bar{2}}{\overline{-1}} & \overline{-1} \end{pmatrix}} = \frac{\bar{7}}{\bar{8}} = \bar{7} \cdot \bar{8} = \overline{56} = \bar{2}$$

A solução possível é  $(\bar{2}, \bar{3}, \bar{2})$

EXEMPLO 23 : RESOLVA O SISTEMA EM  $\mathbb{Z}_6$

$$\begin{cases} -x - \bar{4}y = \bar{0} \\ \bar{3}x + \bar{2}y = \bar{5} \end{cases}$$

TEMOS QUE

$$\begin{pmatrix} -\bar{1} & -\bar{4} \\ \bar{3} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \bar{0} \\ \bar{5} \end{pmatrix}$$

$$\text{Det} \begin{pmatrix} -\bar{1} & -\bar{4} \\ \bar{3} & \bar{2} \end{pmatrix} = \bar{-2} + \bar{12} = \bar{4} + \bar{12} = \bar{16} = \bar{4}$$

$$\text{Det} \begin{pmatrix} \bar{0} & -\bar{4} \\ \bar{5} & \bar{2} \end{pmatrix} = \bar{0} + \bar{20} = \bar{20} = \bar{2}$$

$$\text{Det} \begin{pmatrix} -\bar{1} & \bar{0} \\ \bar{3} & \bar{5} \end{pmatrix} = \bar{-5} - \bar{0} = \bar{1}$$

Agora encontraremos o inverso de  $\bar{4}$  em  $\mathbb{Z}_6$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$

Nesse caso como o  $\bar{4}$  não possui inverso no  $\mathbb{Z}_6$  então vamos analisar os possíveis valores de  $x$  e  $y$ .

Para determinar os valores de  $x$  e  $y$  temos que avaliar através da regra de Cramer os possíveis valores por eles assumidos. Temos então que:  $\det M = \det A \cdot x$  e  $\det N = \det A \cdot y$

Os valores assumidos em  $x$  são:

$$\bar{4} \cdot x = \bar{2}$$

Portanto  $x$  só poderá ser  $\bar{2}$  ou  $\bar{5}$

Os valores assumidos em  $y$  são:

$$\bar{4} \cdot y = \bar{1}$$

Portanto  $y$  não admitirá valores no  $\mathbb{Z}_6$

Temos então que os valores para este Sistema é impossível (SI).

## 7 CONCLUSÃO

Um dos conceitos centrais na matemática é o estudo de sistemas lineares, que são conjuntos de equações lineares envolvendo as mesmas variáveis. Esses sistemas são amplamente utilizados em diversos campos, como engenharia, física e economia, devido à sua aplicabilidade prática. Em alguns casos, é necessário resolver sistemas lineares em um conjunto de números específico, como o conjunto dos números inteiros módulo  $m$ , também conhecido como  $\mathbb{Z}_m$ . Nesses casos, a Regra de Cramer pode ser aplicada para encontrar as soluções do sistema.

A Regra de Cramer é uma técnica poderosa utilizada para resolver sistemas lineares. Ela é baseada na determinante da matriz dos coeficientes do sistema e das determinantes das matrizes obtidas substituindo uma coluna da matriz dos coeficientes pelos termos independentes do sistema. No entanto, quando aplicamos a Regra de Cramer no  $\mathbb{Z}_m$ , precisamos fazer algumas adaptações.

A aplicação da Regra de Cramer no  $\mathbb{Z}_m$  pode simplificar a resolução de sistemas lineares em conjuntos específicos, como o conjunto dos  $\mathbb{Z}_m$ . Essa técnica oferece uma abordagem clara e direta para encontrar as soluções do sistema, desde que o módulo inverso exista para todos os coeficientes do sistema.

Em resumo, a Regra de Cramer é uma ferramenta muito útil para resolver sistemas lineares e, quando aplicada no  $\mathbb{Z}_m$ , oferece uma solução precisa para sistemas nesse conjunto numérico específico. É importante lembrar que a existência do módulo inverso é essencial para aplicação da Regra de Cramer no  $\mathbb{Z}_m$ , caso esse inverso não exista a solução para este sistema linear poderá ser indeterminada ou impossível a depender dos valores obtidos para as incógnitas a serem encontradas através da regra de Cramer ( $\det A \cdot \det X_n = \det M_n$ ). Portanto, ao utilizar essa técnica, é necessário verificar se o conjunto dos  $\mathbb{Z}_m$  permite a resolução do Sistema.

## Referências

- [1] **Boldrini, José Luiz et al** Álgebra Linear, São Paulo: Harbra, 1984.
- [2] **Hoffman, Kenneth. Kunze, Ray.** Álgebra Linear. Formas Bilineares Simétricas: Livros Técnicos e Científicos, Rio de Janeiro, 1979.
- [3] **Manfield, Daniel F. Wilderger, N. J.** Plimpton 322 is Babylonian exact sexagesimal trigonometry: Elsevier Inc, número 44, p. 395-419, August, Sydney, 2017.
- [4] **Morgado, José. Franco de.** Algumas equações diofantinas. Boletim da SBM, número 15, p24-35, Jan/Fev, 1990. Disponível em: <<http://natilus.s.uc.pt/psbm/revista/15/024-035.300.pdf>>. Acesso em 12 de Dez 2019.
- [5] **Natário. José.** Espaço Tempo de Minkowski: A Física como Geometria. Gazeta Matemática, número 162, p 34-36, Nov. 2010. Disponível em: <http://gazeta.spm.pt/getArtigo?gid = 305> >. Acesso em 20 de Fev 2020.
- [6] **OBMEP.** Banco de Questões. Disponível em: <http://www.obmep.org.br/banco.htm>> Acesso em: 20 de Mar 2020.
- [7] **O'Connor, J. J. Robertson, E. F., Hermann Minkowski.** Disponível em: <https://mathshistory.st-andrews.ac.uk/Biographies/Minkowski/>. Acesso em 29 de Fev 2019.
- [8] **Shokranian, Salahoddin. et al.** Teoria dos Números : UnB, Brasília 1999.
- [9] **Hefez, Abramo.** Elementos da Aritmética, Rio de Janeiro: SBM , Rio de Janeiro 2011.

- [10] **SHOKRANIAN, S.** Álgebra I. Rio de Janeiro: Ciência Moderna, 2010.
- [11] **ZAHN, M.** Introdução à Álgebra. Rio de Janeiro: Editora Moderna LTDA, 2013. Hermann Minkowski. Disponível em: <https://mathshistory.st-andrews.ac.uk/Biographies/Minkowski/>. Acesso em 29 de Fev 2019.
- [12] **Oliveira, A. J. Franco de.** Breve introdução histórica e alguns problemas e conjecturas. Boletim da SBM, número 6, p 49-64, outubro, 1993. Disponível em: <http://natilus.s.uc.pt/psbm/revista/6/049-064.300.pdf>. Acesso em 10. Dez 2020.
- [13] **LEQUAIN, Y. e GARCIA, A.** Elementos de Álgebra. 6<sup>a</sup> ed. Rio de Janeiro: IMPA, 2015.