UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Congruências modulares, corpos finitos e aplicações

Jefson dos Santos

Orientador: Dr. Zaqueu Alves Ramos

São Cristóvão, 2015.

Jefson dos Santos

Congruências modulares, corpos finitos e aplicações

Dissertação apresentada ao Departamento de Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Orientador: Dr. Zaqueu Alves Ramos

São Cristóvão, 2015

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Santos, Jefson dos
S237c Congruências modulares, corpos finitos e aplicações / Jefson dos Santos ; orientador Zaqueu Alves Ramos. – São Cristóvão, 2015.
54 f.

Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Sergipe, 2015.

1. Congruência e restos. 2. Corpos finitos. 3. Aritmética modular. I. Ramos, Zaqueu Alves, orient. II. Título.

CDU 511.22

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Congruências modulares, corpos finitos e aplicações.

por

Jefson dos Santos

Aprovada pela Banca Examinadora:

Prof. Dr. Zaqueu Alves Ramos- UFS
Orientador

Prof. Dr. Gerson Cruz Araújo- UFS
Primeiro Examinador

Profª. Dra. Crislene Santos da Paixão - IFS
Segundo Examinador

São Cristóvão, 13 de Abril de 2015.

Agradecimentos

Primeiramente a Deus por ter me dado sabedoria e paciência durante esses dois anos de esforço e dedicação.

A minha mãe, Josefa Rodrigues dos Santos(Dona Jô), pelo sacrifício de me proporcionar a melhor educação que eu poderia ter tido e sempre ter me orientado para que eu buscasse o caminho do conhecimento, além de suas orações que trazem Espíritos de Luz a me proteger.

A Fábio Fontes Vilanova, por suas aulas de Aritmética que me trouxeram até aqui.

À Simone Carla Silva S Evangelista e Rafael Messias Santos, por dividirem momentos decisivos de horas de estudo.

Ao meu orientador, Professor Dr. Zaqueu Alves Ramos, um professor à frente do seu tempo, um garoto dedicado, competente e humildade, cujo exemplo é espelho a ser seguido.

À Engenheira Samia Figueiredo Dorpinghaus, por seu apoio técnico e científico.

A Marcio Monte Alegre Sousa, por ter feito a minha inscrição no PROFMAT.

A Francisco Silva de Azevedo(Chicão), pelas orientações sábias e decisivas.

A Ávido Sadote Barros e Weligton Batista Luz, pelos incentivos e contribuições incondicionais.

Aos professores Almir Rogério, Danilo Felizardo, Humberto, Débora Lopes, Evilson Vieira, Anderson, Kalasas, Naldisson Santos, Allyson que compartilharam dos seus conhecimentos acadêmicos em prol da nossa evolução profissional.

Aos meus colegas de curso pelos momentos de estudos, aflições, alegrias, brincadeiras e o mais importante pela troca de experiência.

À Sociedade Brasileira de Matemática (SBM) pela iniciativa de promover o mestrado profissional cujo objetivo é priorizar a capacitação dos professores de matemática da Educação Básica.

Enfim, a todos que contribuíram diretamente e indiretamente para a concretização deste sonho.

Resumo

Neste trabalho estudamos as congruências modulares com vistas a algumas de suas aplicações. Outra vertente explorada é o entrelaçamento existente entre as congruências modulares e os corpos finitos. Mostraremos, entre outros resultados, que a estrutura de um corpo finito é completamente determinada por sua cardinalidade. Também exibiremos uma aplicação lúdica para os corpos finitos através do chamado *jogo do solitário* (ou, *resta um*).

Palavras Chave: Congruências modulares, corpos finitos, característica, jogo do solitário.

Abstract

In this study we are evaluating the modular congruencies related to some of its application fields. Another important aspect explored is the existing relationship between the modular congruencies and the finite fields. We will show among other results that the structure of a finite field is completely determined by its cardinality. We will also display a ludic application for the finite field through the so called solitary games.

Keywords: Modular congruencies, finite field, characteristic, solitary games.

Sumário

Introdução

Para que serve a matemática? Ainda existe matemática a ser produzida? Estas são perguntas as quais professores que lecionam esta disciplina são frequentemente confrontados. Para respondê-las de forma honesta, satisfatória e atualizada só há um caminho, o da pesquisa incessante, dedicada e, por que não, apaixonada! É preciso que o professor extrapole horizontes, e possa se utilizar de diversos saberes para defender sua matéria e responder os questionamentos da sociedade com conhecimento de causa. Nesse sentido de ir além como professor/pesquisador, é que iniciamos este trabalho sobre congruências modulares e corpos finitos.

Segundo relatos históricos, a ideia de congruência modular foi inventada por Gauss, que observou o uso frequente na aritmética inteira de frases do tipo " *a dá o mesmo resto que b quando dividido por m*". De lá para cá, desenvolveram-se vários resultados a partir dessa noção os quais permitiram, entre outras coisas, um melhor entendimento de questões relacionadas a teoria dos números.

Um fato notável da noção de congruência modular é que ela permite particionar o conjunto dos números inteiros numa coleção finita de subconjuntos. Nesta coleção finita podemos, de forma natural, somar e multiplicar os seus elementos e a aritmética resultante se assemelha com a de $\mathbb{Z}$. Em condições especiais, a multiplicação tem a propriedade de elemento inverso e é nesse ponto que as congruências se conectam com os corpos finitos.

Para contar um pouco da história das congruências modulares e dos corpos finitos de forma mais detalhada, dividimos o texto em quatro capítulos os quais passamos a descrever brevemente.

No Capítulo 1 iniciamos fazendo um breve histórico para situar onde e como a noção de corpo surge. Em seguida apresentamos as definições mais básicas associadas a teoria de corpos como por exemplo: subcorpo, homomorfismo e isomorfismo.

No Capítulo 2 apresentamos a definição de congruência modular e a partir dela chegamos ao conjunto dos restos de divisão por n, aqui denotado por $\mathbb{Z}_n$. Mostramos

que este conjunto possui operações de adição e multiplicação que lhe conferem uma aritmética semelhante à de $\mathbb{Z}$ e que quando n é primo este é um corpo. Encerrando o capítulo apresentamos algumas aplicações em que a aritmética de $\mathbb{Z}_n$ é utilizada.

No terceiro e último Capítulo nos ocupamos em determinar a estrutura dos corpos finitos. Para isso, iniciamos definindo a noção de característica e mostrando que os corpos finitos possuem necessariamente caraterística prima. À custa dessa noção, mostramos o quão restritiva é a hipótese de um corpo ser finito, através do resultado que informa que a cardinalidade de um corpo é necessariamente a potência de um número primo. O principal resultado do capítulo é a classificação dos corpos finitos a menos de isomorfismos. Finalizando, apresentamos uma aplicação bem curiosa dos corpos finitos para resolver certas perguntas referentes ao jogo do solitário.

Capítulo 1

Generalidades sobre corpos

Nesse capítulo faremos uma breve apresentação da noção de corpo, exibindo exemplos e conceitos básicos associados a esta estrutura.

1.1 Um breve histórico

A área da matemática que hoje conhecemos como álgebra tem sua origem no estudo de equações. Contudo, com o passar do tempo esta área tornou-se bastante abrangente e, para entender essa amplitude, fez-se necessário a distinção em períodos *clássico* e *moderno* da álgebra.

O período clássico compreende o intervalo de tempo que inicia em 1700 a.C. e se encerra em 1700 d.C., aproximadamente. Durante esse tempo encontramos a criação gradativa dos símbolos e a resolução de equações quadráticas, cúbicas e de grau quatro. No decorrer desse período a notação algébrica evolui da retórica (verbal) passando pela sincopada (palavras abreviadas) até a simbólica.

O período moderno inicia no final do século dezenove. Esta era uma época em que as palavras *abstração* e *axiomática* estavam em destaque. Por exemplo:

- Em 1882 Pash lança os axiomas da geometria projetiva, expressando pela primeira vez a importância de noções não definidas.

- Em 1883 Cantor defini os números reais como classes de equivalência de sequências racionais de Cauchy.

- Em 1889 Peano fornece seus axiomas para os números naturais.

Essa tendência da época acaba influenciando a álgebra e esta passa a se ocupar em estudar as chamadas *estruturas algébricas*, sendo esse o principal diferencial entre os períodos clássico e moderno. Entre as diversas estruturas algébricas que surgem nessa nova fase da álgebra temos a de grupo, de espaço vetorial, de anel, de módulo e de corpo.

A evolução da teoria de corpos alcança um período de cerca de 100 anos, começando nas décadas iniciais do século dezenove. De fato, elementos dessa teoria já apareciam de forma implícita nos trabalhos sobre resolubilidade de equações por radicais de Evarist Galois e Niels Henrik Abel, nas décadas iniciais do século dezenove. Mais tarde, Dedekind (1871) e Kronecker (1881) realizam estudos em que também figura a ideia de corpo. Nos trabalhos de Dedekind essa ideia ocorre quando ele considera subconjuntos dos números reais ou complexos que são fechados para as quatro operações. Já para Kronecker, ela surge através dos conjuntos de funções racionais, quando ele imagina estes conjuntos equipados com operações de adição e multiplicação.

A primeira definição abstrata de corpo surge em 1893, em um artigo de Heinrich Weber intitulado "*General foundations of Galois theory of equations*". Em sua definição, Weber pressupõe a noção de grupo e a enuncia da seguinte maneira:

> Um grupo faz-se um corpo se dois tipos de composição são possíveis nele, a primeira das quais pode ser chamada de *adição*, a segunda de *multiplicação*. Além disso:
>
> 1. Supomos que ambos tipos de composição são comutativos.
> 2. A adição satisfaz as condições que definem um grupo.
> 3. A multiplicação é tal que
>
> $a(-b) = -(ab)$
> $a(b + c) = ab + ac$
> $ab = ac$ implica $b = c$, a menos que $a = 0$.
> Dados b e c, $ab = c$ determina a, a menos que $b = 0$.

Embora nessa formulação de Weber a lei da associatividade seja omitida e os axiomas não sejam independentes, esta definição está claramente muito perto da que conhecemos atualmente.

O último maior evento nesse processo de evolução da noção de corpo é dado por Ernst Steinitz, em um artigo chamado de "*Algebraische Theorie der Körper*". Embora

Weber tenha sido o primeiro a definir abstratamente a noção de corpo, foi Steinitz o primeiro a estudá-la abstratamente, definindo propriedades importantes como: corpo primo, corpo perfeito, grau de transcendência e extensão de corpo. Este trabalho de Steinitz acabou influenciando vários outros matemáticos, como nos revelam os seguintes depoimentos:

"Steinitz's paper was the basis for all (algebraic) investigations in the school of Emmy Noether" (van der Waerden [6]).

Steinitz's work marks a methodological turning point in algebra, leading to ... 'modern' algebra (Purkert & Wussing [7]).

[Steinitz's work] ... "*can be considered as having given birth to the actual concept of Algebra*" (Bourbaki [8]).

1.2 Definição e primeiros exemplos

A grosso modo, podemos dizer que um corpo é uma estrutura algébrica constituída por um conjunto não vazio e duas operações que satisfazem as propriedades da aritmética elementar. De maneira mais precisa, a definição é como segue.

Definição 1.2.1. Seja $\mathbb{K}$ um conjunto não vazio. Considere $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ e $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ duas operações em $\mathbb{K}$ chamadas respectivamente de *adição* e *multiplicação* de $\mathbb{K}$. Diremos que a terna $(\mathbb{K}, +, \cdot)$ é um *corpo* se as operações gozarem das propriedades a seguir.

P1. **A adição é associativa**: quaisquer que sejam $a, b, c \in \mathbb{K}$ tem-se $(a + b) + c = a + (b + c)$.

P2. **A adição é comutativa:** quaisquer que sejam $a,\ b \in \mathbb{K}$, $a + b = b + a$.

P3. **Existe elemento neutro para a adição:** existe $0 \in \mathbb{K}$ tal que para qualquer $a \in \mathbb{K}$, $0 + a = a$.

P4. **Existência do elemento inverso para a adição:** para cada $a \in \mathbb{K}$ existe $-a \in \mathbb{K}$ tal que $a + (-a) = 0$.

P5. **A multiplicação é associativa:** quaisquer que sejam $a, b, c \in \mathbb{K}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

P6. **A multiplicação é comutativa**: quaisquer que sejam $a, b \in \mathbb{K}$, tem-se $a \cdot b = b \cdot a$.

P7. **Existência do elemento neutro para a multiplicação**: existe $1 \in \mathbb{K}$ tal que para cada $a \in \mathbb{K}$ temos $1 \cdot a = a$.

P8. **Existência do elemento inverso para a multiplicação:** para cada $a \in \mathbb{K} - \{0\}$ existe $a^{-1} \in \mathbb{K}$ tal que $a \cdot a^{-1} = 1$.

P9. **A multiplicação é distributiva com relação à adição**: quaisquer que sejam $a, b, c \in \mathbb{K}$, tem-se $a \cdot (b + c) = a \cdot b + a \cdot c$.

Como percebemos da definição, a estrutura de corpo é determinada pelo conjunto $\mathbb{K}$ e as operações de adição e multiplicação. Assim, pode-se obter corpos distintos com o mesmo conjunto $\mathbb{K}$, bastando para isso definir operações de adição e multiplicação distintas. Desse modo, a rigor, toda vez que nos referíssemos a um corpo deveríamos fazê-lo explicitando toda a terna $(\mathbb{K}, +, \cdot)$. Contudo, quando as operações estão bem entendidas pelo contexto, é comum utilizarmos apenas o conjunto $\mathbb{K}$ para designar toda a estrutura.

Um instante de reflexão e rapidamente podemos nos dar conta que $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são exemplos particulares de corpos. Em contrapartida, também notamos facilmente que $\mathbb{Z}$ não é corpo, uma vez que seus elementos, a menos de -1 e 1, não possuem inverso com respeito a multiplicação.

Por vezes, é interessante reconhecer em um corpo subestruturas que se assemelhem a ele. Tais subestruturas são o motivo da definição que segue.

Definição 1.2.2. Seja $\mathbb{K}$ um corpo. Um subconjunto $\mathbb{K}'$ de $\mathbb{K}$ é dito *subcorpo* de $\mathbb{K}$ se satisfaz as seguintes condições.

(a) Os elementos neutros da adição e multiplicação de $\mathbb{K}$ pertencem a $\mathbb{K}'$.

(b) $\mathbb{K}'$ é fechado para a adição, ou seja, se $a, b \in \mathbb{K}'$ então $a + b \in \mathbb{K}'$.

(c) $\mathbb{K}'$ é fechado para a multiplicação, ou seja, se $a, b \in \mathbb{K}'$ então $a \cdot b \in \mathbb{K}'$.

(d) Para cada $a \in \mathbb{K}'$, $-a \in \mathbb{K}'$.

(e) Para cada $a \in \mathbb{K}' - \{0\}$, $a^{-1} \in \mathbb{K}'$.

É imediato observar que ao restringirmos as operações de $\mathbb{K}$ ao conjunto $\mathbb{K}'$ tem-se que $\mathbb{K}'$ é também um corpo.

Abaixo temos uma cadeia de corpos e subcorpos,

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

A *cardinalidade de um corpo* $(\mathbb{K}, +, \cdot)$ é a cardinalidade do conjunto $\mathbb{K}$. Assim, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são exemplos de corpos cuja cardinalidade é infinita. A pergunta natural é se existem exemplos de corpos cuja cardinalidade seja finita. De fato, como veremos no Capítulo 2 a resposta a esta questão é positiva e chamamos estes corpos de cardinalidade finita de *corpos finitos*.

1.3 "Igualdade" entre corpos

Em matemática, dada uma coleção de objetos de uma mesma estrutura (e.g., a coleção de todos os corpos) uma maneira eficaz de estudar tal coleção é separando-a em partes de modo que os membros de cada parte sejam "iguais" em um certo sentido. Nessa seção, explicaremos em qual sentido dois corpos podem ser ditos "iguais". Para isso, necessitamos inicialmente da seguinte noção.

Definição 1.3.1. Sejam $\mathbb{K}$ e $\mathbb{K}'$ corpos. Uma aplicação $\varphi : \mathbb{K} \to \mathbb{K}'$ é dita um *homomorfismo de corpos* de $\mathbb{K}$ em $\mathbb{K}'$ se

$$\varphi(1) = 1,$$

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

e

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b),$$

para cada $a, b \in \mathbb{K}$.

Exemplo 1.3.2. Dado um corpo $\mathbb{K}$, a aplicação $\mathrm{id}_{\mathbb{K}} : \mathbb{K} \to \mathbb{K}$ definida por $\mathrm{id}_{\mathbb{K}}(a) = a$ (para cada $a \in \mathbb{K}$) é chamada *aplicação identidade* de $\mathbb{K}$. Temos da definição dessa aplicação as seguintes igualdades:

$$\mathrm{id}_{\mathbb{K}}(1) = 1,$$

$$\mathrm{id}_{\mathbb{K}}(a+b) = a+b = \mathrm{id}_{\mathbb{K}}(a) + \mathrm{id}_{\mathbb{K}}(b)$$

e

$$\mathrm{id}_{\mathbb{K}}(a \cdot b) = a \cdot b = \mathrm{id}_{\mathbb{K}}(a) \cdot \mathrm{id}_{\mathbb{K}}(b),$$

para cada $a, b \in \mathbb{K}$. Portanto, $\mathrm{id}_{\mathbb{K}}$ é um homomorfismo de $\mathbb{K}$ em $\mathbb{K}$.

Exemplo 1.3.3. A conjugação complexa $- : \mathbb{C} \to \mathbb{C}$ é um homomorfismo de $\mathbb{C}$ em $\mathbb{C}$. De fato, como sabemos desde o ensino médio:

$$\overline{1} = 1,$$

$$\overline{z+z'} = \overline{z} + \overline{z'}$$

e

$$\overline{z \cdot z'} = \overline{z} \cdot \overline{z'},$$

para cada $z, z' \in \mathbb{C}$.

A seguir catalogamos algumas propriedades fundamentais dos homomorfismos de corpos.

Proposição 1.3.4. *Seja $\varphi : \mathbb{K} \to \mathbb{K}'$ um homomorfismo de corpos. Então,*

(a) $\varphi(0) = 0$.

(b) *Para cada $a \in \mathbb{K}$, $-\varphi(a) = \varphi(-a)$.*

(c) *Para cada $a \in \mathbb{K}$ não nulo temos que $\varphi(a)$ é não nulo e $\varphi(a)^{-1} = \varphi(a^{-1})$.*

(d) *φ é injetor.*

(e) $\mathrm{Im}(\varphi)$ *é um subcorpo de $\mathbb{K}'$.*

Prova.

(a) Ora, $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$; logo $\varphi(0) = 0$.

(b) Dado $a \in \mathbb{K}$ temos $0 = \varphi(0) = \varphi(a-a) = \varphi(a) + \varphi(-a)$; logo, o inverso aditivo de $\varphi(a)$ é $\varphi(-a)$, ou seja $-\varphi(a) = \varphi(-a)$.

(c) Dado $a \in \mathbb{K}$ não nulo temos $1 = \varphi(1) = \varphi(a \cdot a^{-1}) = \varphi(a)\varphi(a^{-1})$. Dessa igualdade segue que $\varphi(a)$ é não nulo, pois caso contrário o produto seria zero, e também segue que seu inverso é $\varphi(a^{-1})$, ou seja, $\varphi(a)^{-1} = \varphi(a^{-1})$.

(d) Suponhamos $a, b \in \mathbb{K}$ tais que $\varphi(a) = \varphi(b)$. Assim, $\varphi(a) - \varphi(b) = 0$. Logo, $\varphi(a - b) = 0$. Pelo item (a) devemos ter $a - b = 0$. Portanto, $a = b$.

(e) A igualdade $\varphi(1) = 1$ nos diz que $1 \in \mathrm{Im}(\varphi)$. Já o item (a) nos diz que $0 \in \mathrm{Im}(\varphi)$. Das igualdades $\varphi(a+b) = \varphi(a)+\varphi(b)$ e $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$, lidas da direita para a esquerda, concluímos que a adição e multiplicação de elementos de $\mathrm{Im}(\varphi)$ permanecem em $\mathrm{Im}(\varphi)$. Finalmente, os itens (b) e (c) nos dão que se um elemento está em $\mathrm{Im}(\varphi)$ então seus inversos aditivos e multiplicativos também pertencem a $\mathrm{Im}(\varphi)$. Portanto, $\mathrm{Im}(\varphi)$ é um subcorpo de $\mathbb{K}'$. □

Finalmente, temos a noção que diz quando dois corpos são "iguais".

Definição 1.3.5. Um homomorfismo de corpos $\varphi : \mathbb{K} \to \mathbb{K}'$ bijetor é chamado de *isomorfismo*. Dois corpos são ditos *isomorfos* se existe um isomorfismo entre eles.

É imediato observar que os exemplos 1.3.2 e 1.3.3 são exemplos de isomorfismos.

Notação: Utilizamos $\mathbb{K} \simeq \mathbb{K}'$ para dizer que $\mathbb{K}$ é isomorfo a $\mathbb{K}'$.

Observação 1.3.6. Em virtude da Proposição 1.3.4 temos que se $\varphi : \mathbb{K} \to \mathbb{K}'$ é um homomorfismo de corpos então $\mathbb{K} \simeq \mathrm{Im}(\varphi)$.

Temos a seguinte propriedade.

Proposição 1.3.7. *Se $\varphi : \mathbb{K} \to \mathbb{K}'$ é um isomorfismo, então a aplicação inversa $\varphi^{-1} : \mathbb{K}' \to \mathbb{K}$ também é um isomorfismo.*

Prova. Notemos que a bijetividade de φ^{-1} é automática. Assim, basta provarmos que φ^{-1} é homomorfismo. Para isso, sejam $c, d \in \mathbb{K}'$. Como φ é sobrejetora, $c = \varphi(a)$ e $d = \varphi(b)$, para convenientes $a, b \in \mathbb{K}$. Note que essas igualdades equivalem respectivamente $a = \varphi^{-1}(c)$ e $b = \varphi^{-1}(d)$. Logo,

$$\varphi^{-1}(c + d) = \varphi^{-1}(\varphi(a) + \varphi(b)) = \varphi^{-1}(\varphi(a + b)) = a + b = \varphi^{-1}(c) + \varphi^{-1}(d)$$

e

$$\varphi^{-1}(c \cdot d) = \varphi^{-1}(\varphi(a) \cdot \varphi(b)) = \varphi^{-1}(\varphi(a \cdot b)) = a \cdot b = \varphi^{-1}(c) \cdot \varphi^{-1}(d).$$

Por outro lado, obviamente $\varphi^{-1}(1) = 1$, já que $\varphi(1) = 1$. Portanto, φ^{-1} é de fato um isomorfismo. □

1.4 O corpo de decomposição de um polinômio

Definimos um polinômio na variável X com coeficientes sobre um corpo $\mathbb{K}$ como sendo uma expressão da forma

$$f(X) = a_0 + a_1X + \ldots + a_nX^n,$$

onde $a_0, \ldots, a_n \in \mathbb{K}$ são chamados *coeficientes* de $f(X)$. Dados polinômios $f(X) = a_0+a_1X+\ldots+a_nX^n$ e $g(X) = b_0+b_1X+\ldots+b_mX^m$ podemos adicioná-los e multiplicá-los de acordo com as seguintes regras: os i-ésimos coeficientes de $f(X) + g(X)$ e $f(X) \cdot g(X)$ são, respectivamente, $(a_i + b_i)$ e $\sum_{r=0}^{i} a_r b_{i-r}$. O polinômio em que todos os coeficientes são nulos é chamado de *polinômio nulo* e o denotamos por 0. O conjunto de todos os polinômios na variável X com coeficientes sobre $\mathbb{K}$ é denotado por $\mathbb{K}[X]$.

Dado um polinômio não nulo $f(X) = a_0 + a_1X + \ldots + a_nX^n$, definimos o seu *grau* como sendo o máximo dos i tais que $a_i \neq 0$. Este número inteiro será denotado por $\mathrm{gr}(f(X))$.

Teorema 1.4.1. *$\mathbb{K}[X]$ equipado das operações definidas acima satisfaz as seguintes propriedades:*

(a) *Quaisquer que sejam $f, g, h \in \mathbb{K}[X]$, $(f + g) + h = f + (g + h)$.*

(b) *Quaisquer que sejam $f, g \in \mathbb{K}[X]$, $f + g = g + f$.*

(c) *Para cada $f \in \mathbb{K}[X]$, $f + 0 = f$.*

(d) *Para cada $f = a_0 + \ldots + a_nX^n \in \mathbb{K}[X]$, $-f := -a_0 - \ldots - a_nX^n \in \mathbb{K}[X]$ é tal que $f + (-f) = 0$.*

(e) *Quaisquer que sejam $f, g, h \in \mathbb{K}[X]$, $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.*

(f) *Quaisquer que sejam $f, g \in \mathbb{K}[X]$, $f \cdot g = g \cdot f$.*

(g) *Para cada $f \in \mathbb{K}[X]$, $f \cdot 1 = f$.*

(h) *Quaisquer que sejam $f, g, h \in \mathbb{K}[X]$, $f \cdot (g + h) = f \cdot g + f \cdot h$.*

Estas propriedades nos mostram que a estrutura determinada por $\mathbb{K}[X]$ e suas operações de adição e multiplicação imitam a estrutura dos inteiros. Além dessas

propriedades, $\mathbb{K}[X]$ também se assemelha a $\mathbb{Z}$ por outra propriedade, chamada algoritmo da divisão.

Teorema 1.4.2 (Algoritmo da divisão)**.** *Sejam $f(X), g(X) \in \mathbb{K}[X]$, com $g(X)$ não nulo. Então,*

(i) *Existem $q(X), r(X) \in \mathbb{K}[X]$ tais que $f(X) = g(X) \cdot q(X) + r(X)$ com $\mathrm{gr(r(X))} < \mathrm{gr(g(X))}$ ou $r(X) = 0$.*

(ii) *Tais polinômios $q(X)$ e $r(X)$ são unicamente determinados.*

Um problema que desperta a curiosidade matemática há séculos diz respeito à determinação de raízes de um polinômio $f(X) \in \mathbb{K}[X]$.

Definição 1.4.3. Seja $\mathbb{K}$ um subcorpo de um corpo L. Dizemos que $\alpha \in L$ é *raiz* de um polinômio $f(X) \in \mathbb{K}[X] - \mathbb{K}$ se $f(\alpha) = 0$.

Uma questão que se põe diante da noção de raiz é:

Questão 1.4.4. *Seja $f(x) \in \mathbb{K}[X] - \mathbb{K}$. Existe um corpo L, tendo $\mathbb{K}$ como subcorpo, tal que f tenha uma raiz em L?*

Como sabemos, pelo teorema fundamental da álgebra, se $\mathbb{K} = \mathbb{R}$ então a resposta a esta questão é afirmativa. De fato, $L = \mathbb{C}$ é um tal corpo. Para responder esta questão de modo geral necessitamos desenvolver algumas preliminares.

Definição 1.4.5. Seja $f(X) \in \mathbb{K}[X] - \mathbb{K}$. Dizemos que $f(X)$ é *irredutível* sobre $\mathbb{K}$ se não existem polinômios $g, h \in \mathbb{K}[X] - \mathbb{K}$ tais que $f(X) = g(X) \cdot h(X)$.

Um fato que torna os polinômios irredutíveis centrais no estudo de $\mathbb{K}[X]$ é:

Teorema 1.4.6 (Fatoração única)**.** *Se $g(X) \in \mathbb{K}[X] - \mathbb{K}$ então $g(X)$ é um produto de polinômios irredutíveis de $\mathbb{K}[X]$. Além disso, esta fatoração é única no seguinte sentido: se*

$$g(X) = p_1(X) \cdots p_r(X) = q_1(X) \cdots q_s(X)$$

com p_j, q_i irredutíveis, então $r = s$ e $p_i = a_i q_i$ com $a_i \in \mathbb{K}$ e $a_i \neq 0$.

Para maiores informações sobre esse resultado consultar, por exemplo, [2, Capítulo IV].

Dado $f(X) \in \mathbb{K}[X]$, definimos uma relação em $\mathbb{K}[X]$ da seguinte maneira: dados $g(X), h(X) \in \mathbb{K}[X]$, $g(X) \sim h(X)$ se, e somente se, $g(X) - h(X)$ é múltiplo de $f(X)$.

É de fácil verificação que $\sim$ definido dessa maneira é uma relação de equivalência em $\mathbb{K}[X]$. A classe de equivalência de um elemento $g(X) \in \mathbb{K}[X]$ será denotada por $\overline{g(X)}$. O conjunto das classes de equivalência de $\mathbb{K}[X]$ pela relação $\sim$ é denotado por $\mathbb{K}[X]/(f(X))$.

Observação 1.4.7. Observe que $g(X) \in \mathbb{K}[X]$ é um múltiplo de $f(X)$ se, e somente se, $\overline{g(X)} = \overline{0}$.

Definimos operações de adição e multiplicação em $\mathbb{K}[X]/(f(x))$ pelas seguintes igualdades:

$$\overline{g(X) + h(X)} := \overline{g(X)} + \overline{h(X)}$$

e

$$\overline{g(X) \cdot h(X)} := \overline{g(X)} \cdot \overline{h(X)}.$$

Estas operações estão bem definidas e conferem a $\mathbb{K}[X]/(f(X))$ as seguintes propriedades:

Teorema 1.4.8. $\mathbb{K}[X]/(f(X))$ *equipado das operações definidas acima satisfaz as seguintes propriedades:*

(a) *Quaisquer que sejam* $\overline{g}, \overline{h}, \overline{p} \in \mathbb{K}[X]/(f(X))$, $(\overline{g} + \overline{h}) + \overline{p} = \overline{g} + (\overline{h} + \overline{p})$.

(b) *Quaisquer que sejam* $\overline{g}, \overline{h} \in \mathbb{K}[X]/(f(X))$, $\overline{g} + \overline{h} = \overline{h} + \overline{g}$.

(c) *Para cada* $\overline{g} \in \mathbb{K}[X]/(f(X))$, $\overline{g} + \overline{0} = \overline{g}$.

(d) *Para cada* $\overline{g} \in \mathbb{K}[X]/(f(X))$, $\overline{g} + (\overline{-g}) = \overline{0}$.

(e) *Quaisquer que sejam* $\overline{g}, \overline{h}, \overline{p} \in \mathbb{K}[X]/(f(X))$, $(\overline{g} \cdot \overline{h}) \cdot \overline{p} = \overline{g} \cdot (\overline{h} \cdot \overline{p})$.

(f) *Quaisquer que sejam* $\overline{g}, \overline{h} \in \mathbb{K}[X]/(f(X))$, $\overline{g} \cdot \overline{h} = \overline{h} \cdot \overline{g}$.

(g) *Para cada* $\overline{g} \in \mathbb{K}[X]/(f(X))$, $\overline{g} \cdot \overline{1} = \overline{g}$.

(h) *Quaisquer que sejam* $\overline{g}, \overline{h}, \overline{p} \in \mathbb{K}[X]/(f(X))$, $\overline{g} \cdot (\overline{h} + \overline{p}) = \overline{g} \cdot \overline{h} + \overline{g} \cdot \overline{p}$.

Além disso, as seguintes condições são equivalentes:

(i) $f(X)$ *é irredutível.*

(ii) $\mathbb{K}[X]/(f(X))$ *é corpo.*

Uma referência para a prova desse teorema é [2, Capítulo IV].

Dado $f(X) \in \mathbb{K}[X]$, com $f(X)$ irredutível, consideremos a aplicação

$$\begin{array}{rccc} \pi: & \mathbb{K}[X] & \to & \mathbb{K}[X]/(f(X)) \\ & g & \mapsto & \overline{g} \end{array}$$

Pela forma em que as operações de adição e multiplicação em $\mathbb{K}[X]/(f(X))$ foram definidas, segue que

$$\pi(1) = \overline{1},$$

$$\pi(g+h) = \pi(g) + \pi(h)$$

e

$$\pi(g \cdot h) = \pi(g) \cdot \pi(h),$$

quaisquer que sejam $g, h \in \mathbb{K}[X]$. Em particular, π restrita a $\mathbb{K}$ é um homomorfismo de $\mathbb{K}$ no corpo $\mathbb{K}[X]/(f(X))$. Pela Proposição 1.3.4 (d), π restrita a $\mathbb{K}$ é um homomorfismo injetor que permite identificarmos $\mathbb{K}$ como subcorpo de $\mathbb{K}[X]/(f(X))$. Dessa maneira é que enxergaremos $\mathbb{K}$ como um subcorpo de $L = \mathbb{K}[X]/(f(X))$.

Com essas informações coletadas podemos agora enunciar o seguinte resultado:

Teorema 1.4.9. *Seja $f(X) \in \mathbb{K}[X] - \mathbb{K}$. Então existe um corpo L contendo $\mathbb{K}$ como subcorpo tal que $f(X)$ possui uma raiz em L.*

Prova. Como dito anteriormente, $f(X)$ se fatora na forma

$$f(X) = p_1(X) \cdots p_r(X),$$

com cada $p_i(X)$ irredutível.

Definamos agora $L = \mathbb{K}[X]/(p_1(X))$ e $\alpha = \overline{X}$. Temos:

$$\begin{aligned} f(\alpha) &= f(\overline{X}) && (1.1) \\ &= \overline{f(X)} && (1.2) \\ &= \overline{0}. && (1.3) \end{aligned}$$

Note que na segunda igualdade foi utilizado a Observação 1.4.7. Portanto, Temos que L é um corpo em que $f(X)$ possui uma raiz, o que conclui a demonstração do teorema. □

Corolário 1.4.10. *Seja $f(X) \in \mathbb{K}[X] - \mathbb{K}$ um polinômio de grau n. Existe um corpo L contendo $\mathbb{K}$ como subcorpo tal que*

$$f(X) = a(X - \alpha_1) \dots (X - \alpha_n),$$

com $a \in \mathbb{K}$ e $\alpha_1, \dots, \alpha_n \in L$.

Prova. Faremos a prova aplicando indução sobre n. Para $n = 1$, temos que $f(X) = aX + b = a(X - \alpha)$, onde $\alpha = -b \cdot a^{-1} \in \mathbb{K}$. Logo, fazendo $L = \mathbb{K}$ temos o desejado.

Agora suponhamos o resultado válido para polinômios de grau $n-1$ ($n > 1$). Pelo teorema anterior temos a existência de um corpo L_1, contendo $\mathbb{K}$ como subcorpo, tal que $f(\alpha_1) = 0$, com $\alpha_1 \in L_1$. Note em particular que podemos ver $f(X)$ como elemento de $L_1[X]$. Utilizando o algoritmo da divisão em $L_1[X]$ temos

$$f(X) = (X - \alpha_1) \cdot g(X),$$

com $g(X) \in L_1[X]$ tendo grau $n-1$. Por hipótese de indução, existe corpo L, contendo L_1 como subcorpo, tal que

$$g(X) = a(X - \alpha_2) \dots (X - \alpha_n),$$

com $a \in L_1$ e $\alpha_2, \dots, \alpha_n \in L$. Em particular, L é um corpo, contendo $\mathbb{K}$ como subcorpo, tal que

$$f(X) = a(X - \alpha_1) \dots (X - \alpha_n).$$

Resta mostrar que $a \in \mathbb{K}$. Mas isso é óbvio quando efetuamos os produtos do lado direito da igualdade e comparamos os coeficientes, usando o fato que $f(X) \in \mathbb{K}[X]$. □

Dado um polinômio $f(X) \in \mathbb{K}[X] - \mathbb{K}$, um corpo mínimo (com respeito a ordem de inclusão), com a propriedade do Corolário 1.4.10, é chamado um corpo de decomposição de $f(X)$ sobre $\mathbb{K}$. Em [4] podemos encontrar o seguinte resultado de unicidade.

Teorema 1.4.11. *Seja $f(X) \in \mathbb{K}[X] - \mathbb{K}$. Se L e L' são corpos de decomposição de $f(X)$ sobre $\mathbb{K}$, então $L \simeq L'$.*

Capítulo 2

Congruências modulares e corpos finitos

Nesse capítulo apresentamos a noção de congruência modular e através dela deduziremos os exemplos mais básicos de corpos finitos. Um fato importante que será verificado, é que os corpos originados da noção de congruência modular são necessariamente de cardinalidade prima. Na última seção do capítulo culminamos com a apresentação de situações do dia-dia em que figuram as congruências modulares.

2.1 Definições e propriedades elementares

A noção de congruência foi estabelecida por Gauss que observou o uso frequente na aritmética inteira de frases do tipo " a dá o mesmo resto que b quando dividido por m". De maneira precisa, a definição é como segue.

Definição 2.1.1. Seja n um número inteiro positivo. Dois números inteiros a e b são *congruentes módulo* n se a diferença $a - b$ é divisível por n.

Notação: Utilizamos o símbolo $a \equiv b \mod n$ para dizer que a é congruente a b módulo n. Caso contrário escreveremos $a \not\equiv b \mod n$.

A respeito da congruência modular temos as seguintes observações:

(a) Como para cada $a \in \mathbb{Z}$, $0 = a - a$ e $n|0$, então $a \equiv a \mod n$. Logo, a relação de equivalência módulo n é *reflexiva*.

(b) Seja $a \equiv b \mod n$. Então $n|a - b$. Em particular, $n| - (a - b)$, ou seja, $n|b - a$. Assim, $b \equiv a \mod n$. Logo, a relação de equivalência módulo n é *simétrica*.

(c) Suponhamos $a \equiv b \mod n$ e $b \equiv c \mod n$. Temos assim que $n|a-b$ e $n|b-c$. Desse modo, $n|(a-b)+(b-c)$, ou seja, $n|a-c$. Assim, $a \equiv c \mod n$. Logo, a relação de equivalência módulo n é *transitiva*.

Segue das conclusões de (a), (b) e (c) que congruência módulo n é uma relação de equivalência. Com isso, podemos falar das classes de equivalência dos elementos de $\mathbb{Z}$ por esta relação. Para cada $a \in \mathbb{Z}$, denotaremos sua respectiva classe por $[a]$ (lembremos que por definição $[a] = \{b \in \mathbb{Z} \mid a \equiv b \mod n\}$). Por outro lado, o conjunto formado pelas classes de equivalência dos elementos de $\mathbb{Z}$ será denotado por $\mathbb{Z}_n$.

Antes da próxima proposição recordamos o seguinte fato: se $\sim$ é uma relação de equivalência em um conjunto A então $a, b \in A$ são tais que $a \sim b$ se, e somente se, as classes de equivalência de a e b são iguais (para estas e outras particularidades sobre relação de equivalência ver, por exemplo, [2, Capítulo 1]).

Proposição 2.1.2. *O conjunto $\mathbb{Z}_n$ é igual a $\{[0], [1], \ldots, [n-1]\}$. Além disso, para cada $0 \leq i, j \leq n-1$, com $i \neq j$, temos $[i] \neq [j]$ (ou seja, a cardinalidade de $\mathbb{Z}_n$ é exatamente n).*

Prova. Primeiro mostraremos que $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$. Para concluirmos essa igualdade é suficiente mostrar que a classe de um elemento $a \in \mathbb{Z}$ é necessariamente igual a classe de um inteiro compreendido entre 0 e $n-1$. Para isso, efetuamos a divisão euclidiana de a por n obtendo

$$a = nq + r,$$

onde $0 \leq r \leq n-1$. Esta igualdade nos dá que $n|a-r$. Logo,

$$a \equiv r \mod n.$$

Logo, $[a] = [r]$ com $0 \leq r \leq n-1$, como desejávamos.

Para a segunda parte da proposição, como $i \neq j$, podemos supor que $j > i$. Assim, $0 < j - i \leq n-1$; logo, n não divide $j-i$; logo, $j \not\equiv i \mod n$; logo $[i] \neq [j]$ como queríamos. □

Observação 2.1.3. A classe de equivalência de um elemento pode ser representada por mais de um elemento. Este fato sutil acaba sendo motivo de confusão quando

lidamos com funções cujo domínio envolve o conjunto $\mathbb{Z}_n$. De fato, em tais situações devemos sempre ter o cuidado de checar se a regra que define a função não depende do representante escolhido, pois caso contrário temos que a função não está bem definida. Para melhor entender o que estamos falando consideremos o seguinte exemplo: suponhamos n um inteiro positivo e f uma regra de $\mathbb{Z}_n$ em $\mathbb{Z}$ que associa a classe $[a]$ ao número inteiro $f([a]) = a$. Por um instante, podíamos pensar que esta regra define uma função. Contudo, este não é o caso. De fato, podemos ver que $[0] = [n]$ mas $f([0]) = 0 \neq n = f([n])$ e, como sabemos, um único elemento do domínio não pode possuir duas imagens distintas.

2.2 Um pouco da aritmética de $\mathbb{Z}_n$

Podemos definir no conjunto operações de adição e multiplicação da maneira mais natural possível. De fato, dados $[a], [b] \in \mathbb{Z}_n$ decretamos que

$$[a] + [b] := [a + b]$$

e

$$[a] \cdot [b] := [a \cdot b].$$

A primeira pergunta diante das definições dessas operações em $\mathbb{Z}_n$ é se realmente elas fazem sentido. Como sabemos, operações são *a priori* funções e, por isso, devem satisfazer as propriedades que definem uma função. Assim, devemos saber se cada par $([a], [b])$ está associado aos únicos elementos $[a] + [b]$ e $[a] \cdot [b]$. Para verificar este fato, suponhamos inteiros a, b, a', b' tais que $[a] = [a']$ e $[b] = [b']$. Temos que $n|a - a'$ e $n|b - b'$. Assim, $n|(a - a') + (b - b')$ ou, equivalentemente, $n|(a + b) - (a' + b')$. Logo, $[a + b] = [a' + b']$, o que mostra que a operação de adição está bem definida. Também concluímos de $n|a - a'$ e $n|b - b'$ que $n|b(a - a')$ e $n|a'(b - b')$. Mas isso nos dá $n|b(a - a') + a'(b - b')$ ou, equivalentemente, $n|ab - a'b'$. Logo, $[ab] = [a'b']$, o que também mostra que a operação de multiplicação está bem definida.

A proposição a seguir nos diz que $\mathbb{Z}_n$ possui propriedades aritméticas semelhantes às dos inteiros.

Teorema 2.2.1. *$\mathbb{Z}_n$ equipado das operações definidas acima satisfaz as seguintes propriedades:*

(a) *Quaisquer que sejam $[a], [b], [c] \in \mathbb{Z}_n$, $([a] + [b]) + [c] = [a] + ([b] + [c])$.*

(b) *Quaisquer que sejam* $[a], [b] \in \mathbb{Z}_n$, $[a] + [b] = [b] + [a]$.

(c) *Para cada* $[a] \in \mathbb{Z}_n$, $[a] + [0] = [a]$.

(d) *Para cada* $[a] \in \mathbb{Z}_n$, $[a] + [-a] = [0]$.

(e) *Quaisquer que sejam* $[a], [b], [c] \in \mathbb{Z}_n$, $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$.

(f) *Quaisquer que sejam* $[a], [b] \in \mathbb{Z}_n$, $[a] \cdot [b] = [b] \cdot [a]$.

(g) *Para cada* $[a] \in \mathbb{Z}_n$, $[a] \cdot [1] = [a]$.

(h) *Quaisquer que sejam* $[a], [b], [c] \in \mathbb{Z}_n$, $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$.

Prova. A prova é consequência do fato que estas propriedades são válidas em $\mathbb{Z}$ e adição e multiplicação comutam com $[\ \ ]$. □

O leitor atento notará, mediante o teorema acima, que $\mathbb{Z}_n$ satisfaz todas as propriedades para ser um corpo com exceção apenas da propriedade referente a existência do elemento inverso para a multiplicação. Na seção a seguir explicaremos em quais situações $\mathbb{Z}_n$ também satisfaz essa propriedade.

2.3 Quando o $\mathbb{Z}_n$ é um corpo?

Na prova do resultado a seguir usaremos o fato da aritmética elementar de que dois números inteiros não nulos a, b tem máximo divisor comum igual a 1 se, e somente se, existem inteiros x, y tais que $ax + by = 1$ (para maiores detalhes sobre esse resultado conferir [3, pag. 96]).

Teorema 2.3.1. *$\mathbb{Z}_n$ é corpo se, e somente se, n é um número primo.*

Prova. Primeiro suponhamos que n é primo. Então, dado um inteiro $1 \leq a \leq n-1$ temos que $\text{mdc}(a, n) = 1$. Logo, existem inteiros x, y tais que $ax + yn = 1$. Assim:

$$[a] \cdot [x] = [a] \cdot [x] + [y] \cdot [n] = [a \cdot x] + [y \cdot n] = [ax + yn] = [1].$$

Isso nos mostra que qualquer elemento em $\mathbb{Z}_n - \{[0]\}$ é invertível. Portanto, $\mathbb{Z}_n$ é corpo.

Reciprocamente, suponhamos que $\mathbb{Z}_n$ é corpo. Para mostrar que n é primo é suficiente mostrarmos que n não é divisível pelos elementos do conjunto $\{2, \ldots, n-1\}$.

Assim, consideremos $a \in \{2, \ldots, n-1\}$. Temos então que $[a] \neq [0]$. Como $\mathbb{Z}_n$ é corpo, existe $[x] \in \mathbb{Z}_n - \{0\}$ tal que $[a][x] = [1]$. Logo, $ax - 1$ é divisivel por n. Logo, existe $y \in \mathbb{Z}$ tal que $ax + yn = 1$. Logo, $\text{mdc}(a, n) = 1$. Logo, a não divide n. Logo, n é primo. □

2.4 Situações do cotidiano em que figuram a aritmética modular

Nesta seção colecionamos algumas situações práticas em que figuram, de maneira natural, a aritmética modular.

2.4.1 A aritmética do calendário

O nosso calendário é denominado de solar por se basear nos movimentos de rotação e translação da terra. O ano solar não é um número inteiro de dias(aproximadamente 365,242199 dias), daí a necessidade dos anos bissextos para uma correção parcial do erro na contagem dos anos. Até 1582 o calendário era o Juliano, que aproximava o ano para 365,25 dias. Ocorre que a diferença entre as duas medidas quando acumulada por 128 anos resultava em aproximadamente um dia a menos. Em 1582, quando o Papa Gregório $XIII$ instituiu o nosso calendário, já havia uma defasagem de 11 dias, segue que o calendário gregoriano determinou:

(A) O dia seguinte ao dia 4 de outubro (quinta-feira), do calendário Juliano, no novo calendário, seria 15 de outubro (sexta-feira).

(B) A cada 4 anos, nos anos múltiplos de 4, haveria um ano bissexto, exceto os centenários que só seriam bissextos se forem múltiplos de 400.

(C) O início do ano passou a ser 1° de Janeiro, e os meses se alternariam com 31 e 30 dias, exceto Fevereiro que teria 28 dias e 29 nos bissextos. O mês de agosto teria 31 dias.

Na sequência desejamos utilizar a aritmética modular para explicitar uma fórmula que permita responder a seguinte questão:

Questão 2.4.1. Em qual dia, $n = 1$ (Domingo), $n = 2$ (Segunda),.., $n = 7$ (Sábado) da semana uma data XX/XX/XXXX irá acontecer?

A fórmula que encontraremos será válida para qualquer ano a partir de 1601, além disso, com o interesse de simplificar a fórmula, o mês de Fevereiro, dada a sua irregularidade de 28 ou 29 dias, será o último mês do ano, logo o 1^o mês do ano, aqui em nossa fórmula, é Março. Portanto, o "ano"da fórmula que será encontrada, tem a seguinte ordem: Março, Abril, Maio, Junho, Julho, Agosto, Setembro, Outubro, Novembro, Dezembro, Janeiro e Fevereiro. Assim, o data 10/02/1967, será, em nossa fórmula, 10/12/1966, e 05/04/1967 será 05/02/1967. Note que 10/02/1967, tem seu ano reduzido para 1966 e seu mês alterado para 12, pois Fevereiro de 1967 é, em nossa consideração, o último mês de 1966. No entanto, em 05/04/1967, modificamos apenas o mês, pois o mês de Abril de 1967, em nossa consideração, corresponde a Fevereiro de 1967.

Usaremos a seguinte notação: d para dia, m para mês e A para quaisquer anos a partir de 1601. Como o dia 01 de Janeiro de 2015 é uma quinta feira e sabemos que 1 corresponde ao Domingo, então a quinta feira é 5, logo $n(1, 11, 2014) = 5$. Portanto, de forma geral, $n(d, m, A)$ é o dia da semana da data (d, m, A).

O dia $n(d, m, A)$ da semana da data (d, m, A) será calculado em três etapas a saber: determinaremos $n(1, 1, A)$, o dia da semana do primeiro dia do mês 1(março) do ano A, depois $n(1, m, A)$, o dia da semana do primeiro dia do mês m do ano A e por fim $n(d, m, A)$.

Observação 2.4.2. Para o cálculo de $n(1, 1, A)$ precisaremos do número de anos bissextos, b, de 1601 até A e, nesse cálculo, denotaremos por $\left[\frac{x}{y}\right]$ o quociente da divisão euclidiana de x por y.

Cálculo do número de anos bissextos desde 1601 até A:

(i) Número de anos múltiplos de 4:

$$\left[\frac{A}{4}\right] - \left[\frac{1600}{4}\right] = \left[\frac{A}{4}\right] - 400.$$

(ii) Número de anos centenários desde 1601 até o ano A:

$$\left[\frac{A}{100}\right] - \left[\frac{1600}{100}\right].$$

(iii) Número de anos centenários bissextos desde 1601 até o ano A:

$$\left[\frac{A}{400}\right] - \left[\frac{1600}{400}\right].$$

(iv) Número de anos centenários que não são bissextos:

$$\left[\frac{A}{100}\right] - \left[\frac{1600}{100}\right] - (\left[\frac{A}{400}\right] - \left[\frac{1600}{400}\right]) = \left[\frac{A}{100}\right] - \left[\frac{A}{400}\right] - 12.$$

Portanto, o número de anos bissextos desde 1601 até o ano A é dado pelo número de anos múltiplos de 4 menos o número de anos centenários não bissextos, donde vem:

$$b = \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] - 388.$$

Seja n o dia da semana de primeiro de março de 1601. Em 1602, que não é bissexto, o primeiro dia de março é um dia após 365 dias. Como $365 \equiv 1 \mod 7$, isso ocorrerá em um dia após n, isto é, $n(1,1,1602) = n+1 \mod 7$, onde a notação ($a \mod 7$) significa o resto da divisão de a por 7. De forma semelhante, para o ano de 1603, o dia primeiro de março é $n(1,1,1603) = n+2 \mod 7$. Em 1604, que é ano bissexto, tem-se que $366 \equiv 2 \mod 7$, logo $n(1,1,1604) = n+2+2 \mod 7$. Ou seja:

$$\begin{aligned}
n(1,1,1602) &= n + 1602 - 1601 + 0 \mod 7,\\
n(1,1,1603) &= n + 1603 - 1601 + 0 \mod 7,\\
n(1,1,1604) &= n + 1604 - 1601 + 1 \mod 7,\\
n(1,1,1605) &= n + 1605 - 1601 + 0 \mod 7.
\end{aligned}$$

Observação 2.4.3. Em 1604(ano bissexto) saímos do padrão dos que não são bissextos, pois contamos 1 e não o zero como nos outros anos, o mesmo vale para os demais anos bissextos, então esse 1 que foge do padrão dos demais, é certamente um contador de anos bissextos desde 1601. Assim sendo, ele nos dá automaticamente o número de anos bissextos b.

Veja,

$$\begin{aligned}
n(1,1,1604) &= n + 1604 - 1601 + 1 \mod 7,\\
n(1,1,1608) &= n + 1608 - 1601 + 1 + 1 \mod 7,
\end{aligned}$$

$$n(1,1,1612) = n + 1612 - 1601 + 1 + 1 + 1 \mod 7,$$

$$n(1,1,1616) = n + 1616 - 1601 + 1 + 1 + 1 + 1 \mod 7,$$

logo, de forma geral, vem

$$n(1,1,A) = n + A - 1601 + b \mod 7.$$

Lembre que consideramos n como o primeiro dia de março de 1601, mas agora, a nossa fórmula está justamente em função desse n, desconhecido até o momento. Portanto, ainda falta calcular n, para que $n(1,1,A) = n + A - 1601 + b \mod 7$ determine o dia da semana do primeiro dia de março de qualquer ano $A > 1600$.

Para calcular n, consultamos o calendário deste ano e verificamos que o dia primeiro de março ocorreu em um Domingo, ou seja, $n(1,1,2015) = 1$. Substituíndo esses dados em $n(1,1,A) = n + A - 1601 + b \mod 7$, vem

$$n(1,1,2015) = n + 2015 - 1601 + \left[\frac{2015}{4}\right] - \left[\frac{2015}{100}\right] + \left[\frac{2015}{400}\right] - 388 \mod 7$$

$$1 = n + 414 + 503 - 20 + 5 - 388 \mod 7$$

$$1 = n + 3 \mod 7.$$

Logo, $n = 5$, uma quinta feira, donde:

$$n(1,1,A) = 5 + A - 1601 + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] - 388 \mod 7$$

$$n(1,1,A) = -1984 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

como

$$-1984 \equiv 4 \mod 7,$$

temos a fórmula que calcula o dia da semana do primeiro dia de março de qualquer ano $A > 1601$, dada por

$$n(1,1,A) = 4 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7.$$

A partir daqui precisamos determinar $n(1,m,A)$ que calcula o dia da semana do primeiro dia do mês m de qualquer ano $A > 1601$.

Para írmos de 1 de Março(que tem 31 dias) para 1 de Abril, somamos 31 dias, mas $31 \equiv 3 \mod 7$, daí $n(1,2,A) = n(1,1,A) + 3 \mod 7$, logo

$$n(1,2,A) = 7 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

e assim sucessivamente somando os números 2 ou 3 ao primeiro dia da semana do mês anterior para obter o primero dia da semana de um determinado mês

$$n(1,3,A) = 9 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

$$n(1,4,A) = 12 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

$$n(1,5,A) = 14 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

$$n(1,6,A) = 17 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

$$n(1,7,A) = 20 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

$$n(1,8,A) = 22 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

$$n(1,9,A) = 25 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7.$$

$$n(1,10,A) = 27 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

$$n(1,11,A) = 30 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

$$n(1,12,A) = 33 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

portanto, os termos constantes 4,7,9,12,14,17,20,22,25,27,30 e 33 são somados à expressão

$$A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

ou seja

$$4, 0, 2, 5, 0, 3, 6, 1, 4, 6, 2, 5 \mod 7.$$

Sabe-se que esses valores $\mod 7$ são produzidos pela seguinte fórmula empírica em função do mês $m = 1, ..., 12$

$$2 + \left[\frac{13m-1}{5}\right].$$

Observação 2.4.4. Se Fevereiro, dada a sua irregularidade de 28 ou 29 dias, não fosse aqui o mês 12, a fórmula empírica estaria comprometida.

Então

$$n(1, m, A) = 2 + \left[\frac{13m-1}{5}\right] + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7.$$

Finalmente, precisamos determinar $n(d, m, A)$, o dia da semana de qualquer mês do ano $A > 1600$ da data (d, m, A).

No decorrer do mês, certamente devemos somar 1 módulo 7 ao dia para obter o seu dia consecutivo, segue imediatamente

$$n(1, m, A) = 1 + 1 + \left[\frac{13m-1}{5}\right] + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

$$n(1+1, m, A) = 1 + 1 + 1 + \left[\frac{13m-1}{5}\right] + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

$$n(1+1+1, m, A) = 1+1+1+1+\left[\frac{13m-1}{5}\right]+A+\left[\frac{A}{4}\right]-\left[\frac{A}{100}\right]+\left[\frac{A}{400}\right] \mod 7,$$

$$n(1+1+1+1, m, A) = 1+1+1+1+1+\left[\frac{13m-1}{5}\right]+A+\left[\frac{A}{4}\right]-\left[\frac{A}{100}\right]+\left[\frac{A}{400}\right] \mod 7,$$

ou seja

$$n(d, m, A) = d + 1 + \left[\frac{13m-1}{5}\right] + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7.$$

(Fórmula publicada por Christian Zeller em 1882).

Exemplo 2.4.5. Qual foi o dia da semana de 10 de janeiro de 1969?

$$n(10, 11, 1968) = 10+1+\left[\frac{13 \cdot 11 - 1}{5}\right]+1968+\left[\frac{1968}{4}\right]-\left[\frac{1968}{100}\right]+\left[\frac{1968}{400}\right] \mod 7.$$

$$n(10, 11, 1968) = 2484 \mod 7 = 6.$$

Portanto, o dia da semana de 10 de janeiro de 1969 foi uma sexta feira.

2.4.2 A aritmética das notas musicais

A cifra musical é definida pelo sistema de notação alfabética em que o nome de cada nota musical corresponde a uma letra de "A" à "G", organizadas tal como as conhecemos para facilitar a memorização: A-lá, B-Si, C-dó, D-ré, E-mi, F-fá e G-sol. Usualmente, não tomamos nessa ordem, mas C-dó, D-ré, E-mi, F-fá, G-sol, A-lá e B-Si. O intervalo entre C-dó e D-ré é de 1 tom, e o menor intervalo possível entre duas notas musicais é de meio (1/2) tom. Dessa maneira concluímos que entre o C e o D existe uma terceira nota que é a nota $C^{\#}$ (dó sustenido), denominada de nota acidentada ou acidente. Entre notas E e F só há (1/2) tom, logo não possuem sustenido, o mesmo ocorre entre as notas B e C. Assim, as notas se dividem em 7 notas naturais (C, D, E, F, G, A e B) e 5 notas acidentadas ($C^{\#}$, $D^{\#}$, $F^{\#}$, $G^{\#}$ e $A^{\#}$). A união delas forma o que definimos como escala cromática das notas musicais ou escala completa:

$$C, C^{\#}, D, D^{\#}, E, F, F^{\#}, G, G^{\#}, A, A^{\#}, B, C.$$

Veja que o C se repetiu após 7 notas naturais (C, D, E, F, G, A, B e C). Esse segundo C, obtido nessa ordem, é denominado de uma oitava acima ou C oitavado, porque avançamos 8 notas naturais (partindo do C) até chegarmos novamente em C. Temos então que uma nota C mais 7 notas naturais nos faz retornar para C, numa visão modular corresponde à $8 \equiv 1 \mod 7$, pois à nota C foram somadas mais 7 notas, logo, temos 8 notas, mas 8 deixa resto 1 na divisão por 7, então voltamos para C. Se a uma nota C somarmos mais 9 notas naturais teremos 10 notas, e 10 deixa resto 3 na divisão por 7, consequentemente subiremos mais três notas partindo do C que serão C, D e chegaremos na nota E, numa visão modular fizemos $10 \equiv 3 \mod 7$.

Exemplo 2.4.6. Qual a décima nona de Ré (ou D)?

$$19 \equiv 5 \mod 7,$$

consequentemente partindo de D avançaremos cinco notas D, E, F e G chegando em A. Assim a resposta é Lá ou A.

Exemplo 2.4.7. Qual a sétima nota de Dó (ou C)?

$$7 \equiv 7 \mod 7,$$

consequentemente partindo de C avançaremos sete notas C, D, E, F, G, A chegando em B. Assim a resposta é Si ou B.

2.4.3 Cifras de HILL

Cifras de Hill é um sistema no qual o texto é dividido em conjuntos de n letras, cada um dos quais é substituído por um conjunto de n letras codificadas (ou cifradas). Portanto, consideremos que cada letra do texto original e do texto codificado, exceto Z, tem um valor numérico que determina sua posição no alfabeto. O valor de Z será zero, pois usaremos congruência $\mod 26$.

Faremos aqui o caso mais simples da Cifra de Hill, transformando pares sucessivos do texto em pares codificados (ou cifrados), de acordo com os passos que se seguem.

(I) Escolheremos uma matriz A de ordem 2 com entradas inteiras, cujas condições serão definidas em seguida.

(II) Agruparemos letras sucessivas do texto em pares, adicionando uma letra fictícia, se o texto possuir uma quantidade ímpar de letras, para completar o último par. Substituiremos cada letra por seu valor, conforme tabela 2.1.

(III) Converteremos cada par sucessivo de letras do texto em um vetor coluna e faremos o produto da matriz obtida no passo (I) pelo vetor coluna, obtendo o vetor cifrado que nos dará o equivalente alfabético.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Tabela 2.1:

Exemplo 2.4.8. Codificaremos "NAO ESPERE POR MIM", utilizando a matriz

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}.$$

Fazendo o agrupamento, conforme o passo (II) temos:

NA OE SP ER EP OR MI MM

Note o acréscimo da letra fictícia M. O seu equivalente pela tabela 2.1 é

$$14\ 1 \quad 15\ 5 \quad 19\ 16 \quad 5\ 18 \quad 5\ 16 \quad 15\ 18 \quad 13\ 9 \quad 13\ 13.$$

Para codificar o par NA, seguindo o passo (III), temos:

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} . \begin{bmatrix} 14 \\ 1 \end{bmatrix} = \begin{bmatrix} 16 \\ 3 \end{bmatrix},$$

que fornece pela tabela 2.1 o texto cifrado PC. Da mesma forma faremos para codificar o par OE:

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} . \begin{bmatrix} 15 \\ 5 \end{bmatrix} = \begin{bmatrix} 25 \\ 15 \end{bmatrix},$$

que fornece pela tabela 2.1 o texto cifrado YO. Porém, quanto ao par SP, surge um problema:

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} . \begin{bmatrix} 19 \\ 16 \end{bmatrix} = \begin{bmatrix} 51 \\ 48 \end{bmatrix}.$$

É imediato que os números 51 e 48 não possuem par equivalente na tabela 2.1. Quando isso acontecer, fica acordado que faremos a congruência módulo 26. Logo,

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} . \begin{bmatrix} 19 \\ 16 \end{bmatrix} = \begin{bmatrix} 51 \\ 48 \end{bmatrix} \text{ ou } \begin{bmatrix} 25 \\ 22 \end{bmatrix},$$

que fornece pela tabela 2.1 o texto cifrado YV.

Colecionando todos os vetores, utilizando esse procedimento, temos a frase cifrada,

PC YO YV OB KV YB EA MM.

O texto do nosso exemplo foi agrupado em pares e criptografado por uma matriz de ordem 2, daí dizermos que a cifra de Hill é 2-cifra de Hill. De forma geral, para uma n-Cifra de Hill agrupamos o texto em conjuntos de n letras e criptografamos com uma matriz de ordem n com entradas inteiras.

Para decodificar as cifras de Hill, utilizaremos a inversa módulo 26 da matriz codificadora, de modo que, se m é um inteiro positivo, diremos que uma matriz A com entradas em $\mathbb{Z}_m$ é invertível módulo m se existir uma matriz B com entradas em $\mathbb{Z}_m$ tal que

$$AB = BA = I \mod m.$$

Proposição 2.4.9. *Uma matriz 2×2 com entradas em $\mathbb{Z}_m$ é invertível módulo m se, e somente se, o resíduo de $det(A)$ módulo m tem um inverso multiplicativo módulo m.*

Prova. Seja $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}_m)$ e $\det(A) = D = ad - bc \in \mathbb{Z}_m$. Suponhamos que a matriz A possua uma inversa multiplicativa módulo m, ou seja, há uma matriz quadrada A^{-1}, com entrada em $\mathbb{Z}_m$, tal que

$$A^{-1} \cdot A = A \cdot A^{-1} = I.$$

Aplicando determinantes,

$$\det(A^{-1}) \cdot \det(A) = \det(A \cdot A^{-1}) = \det(I) = 1 \mod m.$$

Logo, $\det(A^{-1})$ é o inverso multiplicativo módulo m de $\det(A)$.

Reciprocamente, suponhamos que $\text{mdc}(m, D) = 1$. Então, existe $D^{-1} \in \mathbb{Z}_m$ tal que $DD^{-1} = 1 \mod m$. Fazendo um verificação direta temos que

$$A^{-1} = \begin{bmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{bmatrix}$$

é a inversa de A. □

Como o resíduo de $\det(A)$ módulo m terá inverso módulo m se, e somente se, este resíduo e m forem coprimos, daí segue.

Corolário 2.4.10. *Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é invertível módulo m se, e somente se, m e o resíduo módulo m do $det(A)$ são coprimos.*

Como os únicos fatores primos de $m = 26$ é 2 e 13, temos

Corolário 2.4.11. *Uma matriz quadrada A com entradas em $\mathbb{Z}_{26}$ é invertível módulo 26 se, e somente se, o resíduo módulo 26 do $det(A)$ não é divisível por 2 ou por 13.*

Se $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ tem entradas em $\mathbb{Z}_{26}$ e se o resíduo $\det(A)$ módulo 26 não é divisível por 2 ou 13, então a inversa de $\det(A) \mod 26$ é dada por

$$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \mod 26.$$

Seja A a matriz invertível com entradas em $\mathbb{Z}_{26}$, $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, seja P um vetor do texto de 2-cifra de Hill $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$, então o vetor C criptografado é dado por

$$C = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \Leftrightarrow C = AP.$$

Sendo A^{-1} a inversa de A módulo 26, torna-se muito simples decifrar C,

$$C = AP$$

$$A^{-1} \cdot C = A^{-1} \cdot A \cdot P$$

$$A^{-1} \cdot C = I \cdot P$$

$$A^{-1} \cdot C = P,$$

ou seja, basta multiplicar, pela esquerda, o vetor C por A^{-1} módulo 26.

Tendo em vista o exemplo que se seguirá vejamos os inversos módulo 26

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Tabela 2.2:

Exemplo 2.4.12. Decodificar o texto criptografado do exemplo 2.4.8

Temos que a inversa de A módulo 26 é dada por

$$A^{-1} = 3^{-1} \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix} = 9 \cdot \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 27 & -18 \\ 0 & 9 \end{bmatrix} = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \mod 26.$$

O texto

PC YO YV WB KV YB EA MM,

tem como equivalente numérico, pela tabela 2.1, a seguinte lista

16 3 25 15 25 22 15 2 11 22 25 2 5 1 13 13.

Logo,

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 16 \\ 3 \end{bmatrix} = \begin{bmatrix} 40 \\ 27 \end{bmatrix} = \begin{bmatrix} 14 \\ 1 \end{bmatrix} \mod 26,$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 25 \\ 15 \end{bmatrix} = \begin{bmatrix} 145 \\ 135 \end{bmatrix} = \begin{bmatrix} 15 \\ 5 \end{bmatrix} \mod 26,$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 25 \\ 22 \end{bmatrix} = \begin{bmatrix} 201 \\ 198 \end{bmatrix} = \begin{bmatrix} 19 \\ 16 \end{bmatrix} \mod 26,$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 11 \\ 22 \end{bmatrix} = \begin{bmatrix} 187 \\ 198 \end{bmatrix} = \begin{bmatrix} 5 \\ 16 \end{bmatrix} \mod 26,$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 25 \\ 2 \end{bmatrix} = \begin{bmatrix} 41 \\ 18 \end{bmatrix} = \begin{bmatrix} 15 \\ 18 \end{bmatrix} \mod 26,$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 13 \\ 9 \end{bmatrix} = \begin{bmatrix} 13 \\ 9 \end{bmatrix} \mod 26,$$

e

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 13 \\ 13 \end{bmatrix} = \begin{bmatrix} 117 \\ 117 \end{bmatrix} = \begin{bmatrix} 13 \\ 13 \end{bmatrix} \mod 26.$$

Pela tabela 2.1 os equivalentes alfabéticos dos vetores obtidos são:

NA OE SP ER EP OR MI MM,

como era de se esperar.

Quebrando a cifra de Hill

Suponha que Ive ("o espião") consegue algum texto comum e a sua codificação correspondente:

OE ES e YO YV.

Com essa informação Ive irá determinar a matriz decodificadora e consequentemente obter acesso às mensagens secretas entre, por exemplo, Alice e Bob.

Em Álgebra Linear uma transformação fica completamente determinada por seus valores em uma base. Seja uma n-cifra de Hill e se $p_1, p_2, ..., p_n$ forem vetores comuns linearmente independentes cujos correspondentes são $Ap_1, Ap_2, ..., Ap_n$, então temos informação suficiente para encontrar a matriz A.

Teorema 2.4.13 (Determinando a Matriz Decodificadora)**.** *Sejam $p_1, p_2, ..., p_n$ vetores comuns linearmente independente e sejam $c_1, c_2, ..., c_n$, os correspondentes vetores cifrados de uma cifra de n-cifra de Hill. Se*

$$P = \begin{bmatrix} p_1^T \\ p_2^T \\ . \\ . \\ . \\ p_n^T \end{bmatrix}$$ *é a matriz $n \times n$ de vetores linha $p_1^T, p_2^T, ..., p_n^T$ e se*

$$C = \begin{bmatrix} c_1^T \\ c_2^T \\ . \\ . \\ . \\ c_n^T \end{bmatrix}$$ *é a matriz $n \times n$ de vetores linha $c_1^T, c_2^T, ..., c_n^T$, então a sequência de operações elementares sobre linhas reduz C a I, transformando P em $(A^{-1})^T$.*

Prova. Pela definição de P e C é imediato $C = PA^T$. Como A é invertível e $p_1, p_2, ..., p_n$ são vetores linearmente independentes, então C é uma matriz invertível.

Sejam $E_1, E_2, ..., E_k$ as matrizes elementares que correspondem às operações elementares com linhas que reduzem C a I, isto é, $E_k \cdots E_1 C = I$, como $C = PA^T$, então temos $E_k \cdots E_1 PA^T = I$, logo

$$E_k \cdots E_1 P = (A^{-1})^T.$$

□

Ou seja, a mesma sequência de operações com as linhas que reduz C a I, converte P a $(A^{-1})^T$. Este teorema diz que para obtermos a matriz transposta da matriz decodificadora, $(A^{-1})^T$, devemos encontrar uma sequência de operações sobre linhas que reduz C a I e aplicar as mesmas operações sobre as linhas de P.

Exemplo 2.4.14. Ive interceptou a mensagem YO YV, e supôs que trata-se, respectivamente, de OE ES. Se ele estiver correto, o que deve fazer para encontrar a matriz decodificadora A^{-1}?

Pela tabela 2.1 temos que YO YV corresponde à 25 15 e 25 22 enquanto OE ES corresponde à 15 5 e 19 16.

Logo,

$$p_1 = \begin{bmatrix} 15 \\ 5 \end{bmatrix} \Leftrightarrow c_1 = \begin{bmatrix} 25 \\ 15 \end{bmatrix}$$

e

$$p_2 = \begin{bmatrix} 19 \\ 16 \end{bmatrix} \Leftrightarrow c_2 = \begin{bmatrix} 25 \\ 22 \end{bmatrix}.$$

A matriz

$$C = \begin{bmatrix} c_1^T \\ c_2^T \end{bmatrix} = \begin{bmatrix} 25 & 15 \\ 25 & 22 \end{bmatrix},$$

será reduzida à matriz identidade por operações elementares sobre linhas e simultaneamente aplicadas também a

$$P = \begin{bmatrix} p_1^T \\ p_2^T \end{bmatrix} = \begin{bmatrix} 15 & 5 \\ 19 & 16 \end{bmatrix},$$

para obter $(A^{-1})^T$. Este procedimento é realizado adjuntando P à direita de C e realizando em seguida uma sequência de operações elementares sobre linhas para reduzir o lado esquerdo à matriz identidade I. Como se segue,

$$\left[\begin{array}{cc|cc} 25 & 15 & 15 & 5 \\ 25 & 22 & 19 & 16 \end{array}\right],$$

multiplicamos a primeira linha por $25^{-1} = 25$,

$$\left[\begin{array}{cc|cc} 1 & 375 & 375 & 125 \\ 25 & 22 & 19 & 16 \end{array}\right],$$

substituímos a primeira linha por seus resíduos módulo 26,

$$\left[\begin{array}{cc|cc} 1 & 11 & 11 & 21 \\ 25 & 22 & 19 & 16 \end{array}\right],$$

trocamos a segunda linha pela primeira multiplicada por -25 somada à segunda,

$$\left[\begin{array}{cc|cc} 1 & 11 & 11 & 21 \\ 0 & -253 & -256 & -509 \end{array}\right],$$

substituímos a segunda linha por seus resíduos módulo 26,

$$\left[\begin{array}{cc|cc} 1 & 11 & 11 & 21 \\ 0 & 7 & 4 & 11 \end{array}\right],$$

multiplicamos a segunda linha por $7^{-1} = 15$,

$$\left[\begin{array}{cc|cc} 1 & 11 & 11 & 21 \\ 0 & 1 & 60 & 165 \end{array}\right],$$

substituímos a segunda linha por seus resíduos módulo 26,

$$\left[\begin{array}{cc|cc} 1 & 11 & 11 & 21 \\ 0 & 1 & 8 & 9 \end{array}\right],$$

trocamos a primeira linha pela segunda multiplicada por -11 somada à primeira,

$$\left[\begin{array}{cc|cc} 1 & 0 & -77 & -78 \\ 0 & 1 & 8 & 9 \end{array}\right],$$

substituímos a primeira linha por seus resíduos módulo 26,

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 8 & 9 \end{array}\right],$$

logo,

$$[A^{-1}]^T = \left[\begin{array}{cc} 1 & 0 \\ 8 & 9 \end{array}\right],$$

portanto, a matriz decodificadora é dada por $A^{-1} = \left[\begin{array}{cc} 1 & 8 \\ 0 & 9 \end{array}\right]$.

Capítulo 3

A estrutura dos corpos finitos

No capítulo anterior apresentamos os primeiros exemplos de corpos finitos, estes oriundos das congruências modulares. Como vimos a cardinalidade desses corpos era necessariamente um número primo. Nesse capítulo, além de mostrarmos que qualquer outro corpo finito está intimamente relacionado com os corpos do capítulo precedente, mostraremos como deve ser a cardinalidade nesse caso e como os corpos finitos são classificados a menos de isomorfismo.

3.1 A característica de um corpo

Na determinação da estrutura de um corpo finito a seguinte noção é de importância fundamental.

Definição 3.1.1. Seja $\mathbb{K}$ um corpo. Consideremos a sequência em $\mathbb{K}$

$$1, 1+1, 1+1+1, \ldots$$

(a) Se todos os termos dessa sequência são não nulos dizemos que $\mathbb{K}$ é um corpo de *característica* 0.

(b) Se esta sequência admite um termo nulo, dizemos que $\mathbb{K}$ é um corpo de *característica* p, onde p é o menor inteiro positivo tal que $\underbrace{1+\ldots+1}_{p \text{ parcelas}} = 0$.

Notação: Para efeito de simplicidade, em um corpo $\mathbb{K}$ denotaremos a soma $\underbrace{1+\ldots+1}_{r \text{ parcelas}}$ por $r \cdot 1$.

Exemplo 3.1.2. $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos de característica zero.

Exemplo 3.1.3. Para cada inteiro primo p, sabemos pelas considerações acima que $\mathbb{Z}_p$ é um corpo de característica p.

Observação 3.1.4. Se dois corpos $\mathbb{K}$ e $\mathbb{K}'$ são isomorfos então eles tem a mesma característica. De fato, isso ocorre pois se $\varphi : \mathbb{K} \to \mathbb{K}'$ é um isomorfismo então $\underbrace{1 + \ldots + 1}_{n \text{ parcelas}}$ é zero se, e somente se, $\varphi(\underbrace{1 + \ldots + 1}_{n \text{ parcelas}}) = 0$. Assim, a característica de um corpo é o que se chama de *invariante* da estrutura de corpos (invariante no sentido de que se mantém igual nos membros de uma mesma classe de equivalência). Em particular, corpos com características distintas não podem ser isomorfos.

A proposição a seguir nos mostra que a característica de um corpo não pode assumir valores inteiros arbitrários.

Proposição 3.1.5. *Seja $\mathbb{K}$ um corpo. Então a característica de $\mathbb{K}$ é 0 ou um número primo.*

Prova. Suponhamos que a característica de $\mathbb{K}$ não seja 0. Então a característica de $\mathbb{K}$ é um inteiro positivo $p > 0$. Devemos mostrar que p é necessariamente um número primo. Para isso, suponhamos o contrário. Então, $p = qr$ com $1 < q, r < p$. Desse modo, $0 = p \cdot 1 = (q \cdot 1)(r \cdot 1)$. Como $\mathbb{K}$ é um corpo, devemos ter $q \cdot 1 = 0$ ou $r \cdot 1 = 0$. Mas como $q, r < p$ temos um absurdo, já que por hipótese p é o menor inteiro positivo tal que $p \cdot 1 = 0$. □

O próximo resultado revela como deve ser a característica de um corpo finito.

Proposição 3.1.6. *Se $\mathbb{K}$ é um corpo finito então sua característica é um número inteiro primo.*

Prova. Pela Proposição 3.1.5, é suficiente provarmos que a característica de $\mathbb{K}$ não é zero. Ou seja, basta exibirmos um número natural r tal que $r \cdot 1 = 0$. Para isso, notemos que a sequência

$$1, 2 \cdot 1, 3 \cdot 1, \ldots, n \cdot 1, \ldots$$

deve ter apenas uma quantidade finita de termos distintos, pois seus termos estão em $\mathbb{K}$ e este é um corpo finito. Logo, existem $s, t \in \mathbb{N}$, com $s \neq t$, tais que $t \cdot 1 = s \cdot 1$. Podemos supor que existe $r \in \mathbb{N}$ tal que $t = r + s$. Logo, $(r + s) \cdot 1 = s \cdot 1$. Assim, $r \cdot 1 + s \cdot 1 = s \cdot 1$. Portanto, $r \cdot 1 = 0$. □

Observação 3.1.7. Seja $\mathbb{K}[X]$ tal como definido na Seção 1.4. Podemos considerar outro conjunto a partir deste como definido na igualdade abaixo:

$$\mathbb{K}(X) := \left\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in \mathbb{K}[X] \text{ e } g(X) \text{ é não nulo} \right\}.$$

Se pensarmos $\mathbb{K}(X)$ equipado com as operações de adição e multiplicação abaixo definidas

$$\frac{f(X)}{g(X)} + \frac{p(X)}{q(X)} := \frac{f(X) \cdot q(X) + p(X) \cdot (g(X))}{g(X) \cdot q(X)}$$

e

$$\frac{f(X)}{g(X)} \cdot \frac{p(X)}{q(X)} := \frac{f(X) \cdot p(X)}{g(X) \cdot q(X)},$$

temos que $\mathbb{K}(X)$ é um corpo. Notemos que $\mathbb{K}(X)$ é infinito independente de quem seja o corpo $\mathbb{K}$. Em particular, $\mathbb{Z}_p(X)$ será um corpo infinito com característica p. Este exemplo nos diz que a recíproca da Proposição 3.1.6 não é verdadeira.

3.2 A cardinalidade de um corpo finito

Nosso primeiro resultado mostra o quanto a hipótese de ser corpo finito é restritiva, pois, como veremos, não podemos ter corpos finitos de cardinalidade arbitrária.

Teorema 3.2.1. *Seja $\mathbb{K}$ um corpo finito de característica p. Então existe um número natural n tal que a cardinalidade de $\mathbb{K}$ é exatamente p^n.*

Prova. Consideremos a aplicação $\varphi : \mathbb{Z}_p \to \mathbb{K}$ definida por

$$\varphi([a]) = a \cdot 1.$$

Afirmamos que φ está bem definida, isto é, não depende de representantes. Para verificar esta afirmação, considere $a, a' \in \mathbb{Z}$ tais que $[a] = [a']$. Então, $p|a - a'$. Logo, $(a - a') \cdot 1 = 0$ ou, equivalentemente, $\varphi([a]) = a \cdot 1 = a' \cdot 1 = \varphi([a'])$. Assim, temos que φ está bem definida.

É imediato observar que φ é homomorfismo. Logo, pela Proposição 1.3.4 (d), φ é injetor.

Denotemos por $\mathbb{K}'$ a imagem de φ. Como φ é injetora, temos que $\mathbb{K}'$ tem exatamente p elementos. Também temos pela Proposição 1.3.4 (e) que $\mathbb{K}'$ é um subcorpo

de $\mathbb{K}$.

Consideremos $\mathfrak{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ um subconjunto de $\mathbb{K}$ satisfazendo as seguintes condições:

(A) Cada elemento de $\mathbb{K}$ se escreve na forma $\alpha_1 \cdot \mathbf{v}_1 + \ldots + \alpha_n \cdot \mathbf{v}_n$ com $\alpha_1, \ldots, \alpha_n \in \mathbb{K}'$.

(B) $\mathfrak{B}$ tem cardinalidade mínima entre todos os subconjuntos de $\mathbb{K}$ que satisfazem a propriedade (A).

Notemos que $\mathbb{K}$ é obviamente um conjunto que satisfaz o item (A). Logo, um conjunto como $\mathfrak{B}$ existe pelo princípio da boa ordenação.

AFIRMAÇÃO: *Cada elemento de* $\mathbb{K}$ *se escreve de forma única como uma soma da forma*

$$\alpha_1 \cdot \mathbf{v}_1 + \ldots + \alpha_n \cdot \mathbf{v}_n,$$

com $\alpha_1, \ldots, \alpha_n \in \mathbb{K}'$.

Para provar esta afirmação, suponhamos um elemento que admita duas escritas distintas, digamos

$$\alpha_1 \cdot \mathbf{v}_1 + \ldots + \alpha_n \cdot \mathbf{v}_n = \alpha_1' \cdot \mathbf{v}_1 + \ldots + \alpha_n' \cdot \mathbf{v}_n,$$

logo,

$$(\alpha_1 - \alpha_1') \cdot \mathbf{v}_1 + \ldots + (\alpha_n - \alpha_n') \cdot \mathbf{v}_n = 0.$$

Como as escritas são distintas, então podemos supor, sem perda de generalidade, que $\alpha_1 - \alpha_1' \neq 0$. Logo,

$$\begin{aligned} \mathbf{v}_1 &= -(\alpha_1 - \alpha_1')^{-1}[(\alpha_2 - \alpha_2') \cdot \mathbf{v}_2 + \ldots + (\alpha_n - \alpha_n') \cdot \mathbf{v}_n] \\ &= \beta_2 \cdot \mathbf{v}_2 + \ldots + \beta_n \mathbf{v}_n \end{aligned} \tag{3.1}$$

onde $\beta_i = -(\alpha_1 - \alpha_1')^{-1}(\alpha_i - \alpha_i')$, para cada $2 \leq i \leq n$ (note que os β_i são elementos de $\mathbb{K}'$ pois são produtos de elementos em $\mathbb{K}'$).

Agora consideremos um elemento arbitrário $\mathbf{v}$ de $\mathbb{K}$. Temos que

$$\mathbf{v} = \gamma_1 \cdot \mathbf{v}_1 + \ldots + \gamma_n \cdot \mathbf{v}_n \tag{3.2}$$

com $\gamma_i \in \mathbb{K}'$, para cada $1 \leq i \leq n$. Substituindo o valor de $\mathbf{v}_1$ nesta igualdade obtemos

$$\mathbf{v} = (\beta_2\gamma_1 + \gamma_2)\mathbf{v}_2 + \ldots + (\beta_n\gamma_1 + \gamma_n)\mathbf{v}_n \tag{3.3}$$

com $\beta_n\gamma_1 + \gamma_n \in \mathbb{K}'$, para cada $2 \leq i \leq n$. Assim, estamos mostrando que $\mathfrak{B}' = \{\mathbf{v}_2, \ldots, \mathbf{v}_n\}$ é um conjunto com $n-1$ elementos que satisfaz a condição (A). Mas isso contraria a minimalidade de $\mathfrak{B}$. Portanto, a afirmação segue.

De posse dessa afirmação segue que para contar a cardinalidade de $\mathbb{K}$ devemos contar a quantidade de listas $(\alpha_1, \ldots, \alpha_n)$ com $\alpha_i \in \mathbb{K}'$ para cada $1 \leq i \leq n$. Como a cardinalidade de $\mathbb{K}'$ é p segue que o número de tais listas deve ser exatamente p^n. □

Lema 3.2.2. *Seja $\mathbb{K}$ um corpo de característica $p > 0$ e a, b elementos de $\mathbb{K}$. Então, para cada número natural n tem-se*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Prova. Primeiro faremos a prova para $n = 1$. Utilizando a expansão binomial tem-se

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \ldots + \binom{p}{r}a^{p-r}b^r + \ldots + \binom{p}{p-1}ab^{p-1} + b^p. \tag{3.4}$$

Notemos que para $1 \leq r \leq p-1$, o coeficiente binomial $\binom{p}{r}$ é um número inteiro maior que 1. Além disso temos

$$\binom{p}{r} \cdot s! = p \cdot (p-1) \cdots (p-(p-s)+1),$$

onde $s = p - r$ ou $s = r$. Em todo caso, $s < p$. Como p é primo, então ele divide algum fator de $\binom{p}{r} \cdot s!$. Mas os fatores de $s!$ são todos menores que p, logo p divide $\binom{p}{r}$. Assim, como o corpo $\mathbb{K}$ tem característica p segue que em (3.4) as parcelas $\ldots + \binom{p}{r}a^{p-r}b^r$ são zero. Logo,

$$(a+b)^p = a^p + b^p,$$

como desejado.

Supondo agora a afirmação verdadeira para $n-1$ temos:

$$(a+b)^{p^n} = [(a+b)^{p^{n-1}}]^p = (a^{p^{n-1}} + b^{p^{n-1}})^p = (a^{p^{n-1}})^p + (b^{p^{n-1}})^p = a^{p^n} + b^{p^n}$$

e assim concluímos a demonstração do lema. □

Nosso propósito a seguir é demonstrar a recíproca do Teorema 3.2.1. Para isso, usaremos os seguinte resultado:

Teorema 3.2.3. *Seja $\mathbb{K}$ um corpo e $f(X) = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{K}[X]$ não nulo. As raízes de $f(X)$ são duas a duas distintas se, e somente se, $mdc(f(X), f'(X)) = 1$, onde $f'(X) = a_1 + 2a_2X + \ldots + na_nX^{n-1}$ (o polinômio $f'(X)$ é chamada a derivada formal de $f(X)$).*

Para a prova desse teorema ver [4, Proposition 5.3.2].

Agora podemos exibir a recíproca do Teorema 3.2.1.

Teorema 3.2.4. *Sejam p, n números inteiros positivos tal que p é primo. Então existe um corpo $\mathbb{K}$, de característica p, com exatamente p^n elementos.*

Prova. Definamos $q = p^n$. Suponhamos $\mathbb{K}$ o corpo de decomposição do polinômio $f(X) = X^q - X$ sobre $\mathbb{Z}_p$. Notemos que $\text{mdc}(f(X), f'(X)) = \text{mdc}(X^q - X, -1) = 1$. Logo, as raízes de $f(X)$ são duas a duas distintas.

Definamos agora $L = \{\alpha \in \mathbb{K} \mid f(\alpha) = 0\}$. Afirmamos que L é um subcorpo de $\mathbb{K}$. Obviamente, $f(0) = 0$ e $f(1) = 0$, logo, $0, 1 \in L$. Agora, suponhamos $\alpha, \beta \in L$. Temos,

$$\begin{aligned} (\alpha + \beta)^q &= \sum_{i=0}^{q} \binom{q}{i} \alpha^{q-i}\beta^i && (3.5) \\ &= \alpha^q + \beta^q && (3.6) \\ &= \alpha + \beta && (3.7) \end{aligned}$$

onde a segunda igualdade ocorre em virtude do Lema 3.2.2. Assim, $\alpha + \beta \in L$. Também temos:

$$(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta,$$

o que nos dá $\alpha\beta \in L$. Por fim, dado $\alpha \in L$ não nulo temos

$$(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}$$

e

$$(-\alpha)^q = -\alpha,$$

ou seja, $\alpha^{-1}, -\alpha \in L$.

Como L contém $\mathbb{Z}_p$ como subcorpo e todas as raízes de $f(X)$ pertencem a L segue que $L = \mathbb{K}$. Como $|L| = \text{gr}(f(X)) = q$, temos o desejado. □

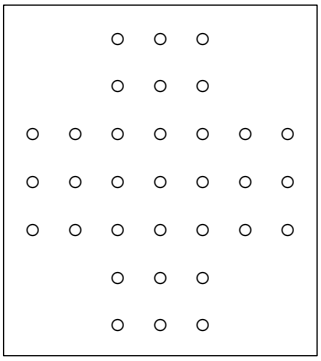
Finalmente, mostraremos que um corpo finito é completamente determinado por sua cardinalidade.

Teorema 3.2.5. *Sejam $\mathbb{K}$ e $\mathbb{K}'$ dois corpos finitos de mesma cardinalidade. Então $\mathbb{K}$ e $\mathbb{K}'$ são isomorfos.*

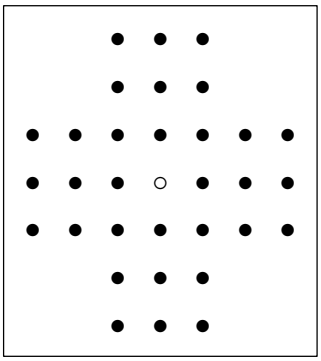
Prova. Do que já foi discutido antes, devem existir inteiros p e n, com p primo, tais que $|\mathbb{K}| = |\mathbb{K}'| = p^n$ e $\text{car}(\mathbb{K}) = \text{car}(\mathbb{K}') = p$. Em particular, $\mathbb{Z}_p$ é subcorpo de $\mathbb{K}$ e $\mathbb{K}'$. Pela demonstração do Teorema 3.2.4 segue que $\mathbb{K}$ e $\mathbb{K}'$ são ambos corpos de decomposição do polinômio $X^{p^n} - X \in \mathbb{Z}_p[X]$. Assim, pelo Teorema 1.4.11, segue que $\mathbb{K} \simeq \mathbb{K}'$. □

3.3 O jogo do solitário

Considere um tabuleiro como ilustrado abaixo.



Em cada buraco do tabuleiro, com exceção do central, colocamos uma bola como mostra a figura a seguir.



O jogo desenvolve-se movimentando uma bola por cima de outra adjacente (na vertical ou horizontal) para um buraco vazio; a bola sobre a qual se saltou é então removida do jogo. O objetivo do jogador é chegar a uma situação em que so reste uma bola no tabuleiro.

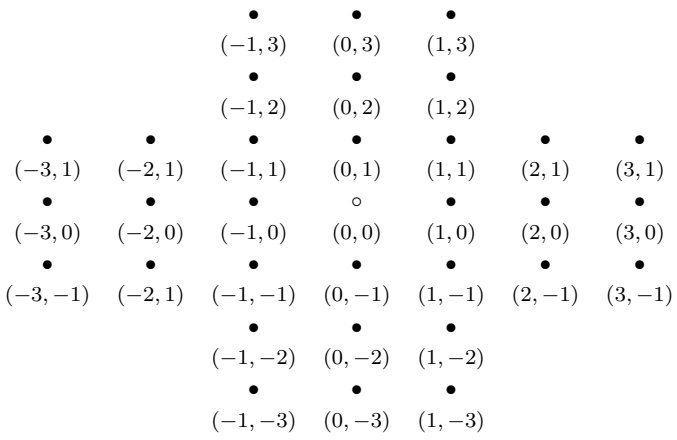
Questão 3.3.1. *Quais são as posições possíveis para esta última bola?*

Para responder a esta questão usaremos o corpo $\mathbb{K}$ com 2^2 elementos. Digamos que $\mathbb{K} = \{0, 1, \alpha, \beta\}$. As tabelas de adição e multiplicação de $\mathbb{K}$ são, respectivamente:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Agora referenciamos os buracos do tabuleiro por pares de inteiros (i, j) da seguinte forma:



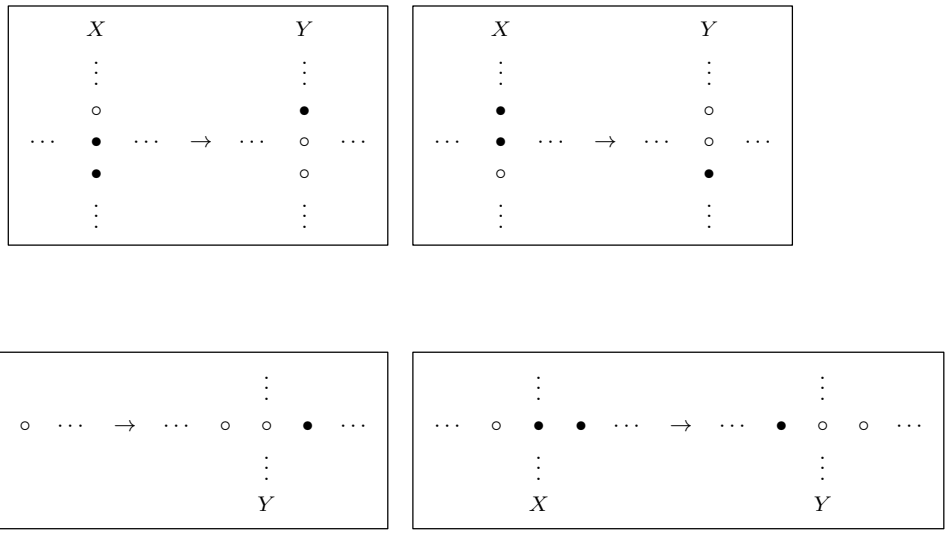
Para cada conjunto X de bolas colocadas no tabuleiro definimos:

$$A(X) = \sum_{(i,j)\in X} \alpha^{i+j}, \qquad B(X) = \sum_{(i,j)\in X} \alpha^{i-j}.$$

Por exemplo, para a posição iniclal X_1 do jogo, temos:

$$\begin{aligned} A(X_1) = B(X_1) &= 2\alpha^4 + 4\alpha^3 + 5\alpha^2 + 4\alpha + 2\alpha^0 + 4\alpha^{-1} + 5\alpha^{-2} + 4\alpha^{-3} + 2\alpha^{-4} \\ &= 0 + 0 + 5\beta + 0 + 0 + 0 + 5\alpha + 0 + 0 \\ &= \alpha + \beta = 1. \end{aligned} \tag{3.8}$$

Cada jogada que transforma um conjunto X de bolas no tabuleiro em um conjunto Y é necessariamente de um dos quatro tipos seguintes:



Claramente, em qualquer desse tipos de jogada temos $A(X) = A(Y)$ e $B(X) = B(Y)$. Por exemplo, no primeiro tipo, se supusermos que a bola a ser movimentada está inicialmente na posição (i, j) e portanto, após a jogada, vai ficar na posição $(i, j + 2)$, então

$$A(X) - A(Y) = \alpha^{i+j} + \alpha^{i+j+1} - \alpha^{i+j+2} = \alpha^{i+j}(1 + \alpha + \alpha^2) = 0$$

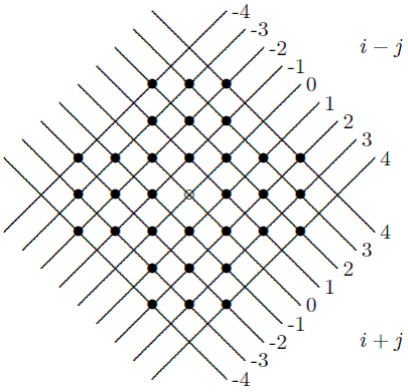
e

$$B(X) - B(Y) = \alpha^{i-j} + \alpha^{i-j-1} - \alpha^{i-j-2} = \alpha^{i-j}(1 + \beta + \beta^2) = 0.$$

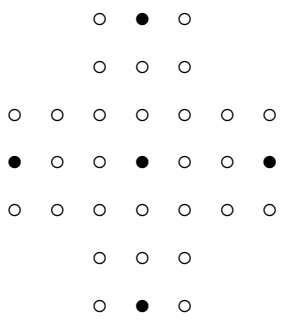
Logo, o par $(A(X), B(X))$ é invariante ao longo do jogo. Assim, se o jogo terminar com uma só bola no tabuleiro, na posição (i, j), teremos necessariamente $A(\{(i, j)\}) = 1$ e $B(\{(i, j)\}) = 1$, isto é, $\alpha^{i+j} = 1$ e $\alpha^{i-j} = 1$. Como as sucessivas potências de α são

$$\alpha^{-4} = \beta,\ \alpha^{-3} = 1,\ \alpha^{-2} = \alpha,\ \alpha^{-1} = \beta,\ \alpha^{0} = 1,\ \alpha^{1} = \alpha,\ \alpha^{2} = \beta,\ \alpha^{3} = 1,\ \alpha^{4} = \alpha,$$

então a posição (i, j) da bola final terá que satisfazer $i + j \in \{-3, 0, 3\}$ e $i - j \in \{-3, 0, 3\}$. Sendo assim, as únicas posições finais possíveis são $(-3, 0)$, $(0, -3)$, $(0, 0)$, $(0, 3)$ e $(3, 0)$.



Logo, as únicas posições, para a possível última bola, são exibidas como segue,



Considerações finais

Aprendemos aqui um pouco mais sobre a diferença entre álgebra moderna e álgebra abstrata. Conhecemos os exemplos mais básicos de corpos finitos através da congruência modular e vimos que a estrutura de um corpo finito é completamente determinada por sua cardinalidade, além disso podemos verificar uma aplicação curiosa de um corpo finito para resolvermos um questionamento do jogo do solitário. Algumas aplicações no cotidiano de congruência modular, foram feitas em linguagem básica e acessível a qualquer estudante do ensino básico.

Portanto, levamos daqui um horizonte mais amplo de conhecimento com noções que podem nos auxiliar em práticas e ações pedagógicas que possam favorecer o nosso trabalho enquanto professor pesquisador .

Referências Bibliográficas

[1] BRUIJN, N., *A solitaire game and its relation to a finite field*, J. Recreational Math. 5 (1972) 133.

[2] GONÇALVES, A., *Introdução à álgebra,* IMPA, Projeto Euclides, 5. ed., Rio de Janeiro, 2008.

[3] HEFEZ, A., *Aritmética*, Coleção PROFMAT. 1 (2013) 330.

[4] COX, D., *Galois Theory*, Wiley, 2 ed, 2012.

[5] KLEINEN, I., *A history of abstract algebra*, Birkhaüser, 2000.

[6] VAN DER WAERDEN, B. L., *Die Algebra seit Galois*, Jahresbericht d. DMV 1966, **68:** 155–165.

[7] PURKERT, W., WUSSING, H., Abstract algebra, in *Companion Encyclopedia of the History and Philosophy of the Mathematical Sciences*, ed. by I. Grattan–Guinness, Routledge, 1994, vol. 1, pp. 741–760.

[8] BOUBARKI, N., *Elements of the History of Mathematics*, Springer–Verlag, 1984.