Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Cripto-Sistemas com Chave Pública Baseado em Extensões Cúbicas

por

Almir César Ferreira Cavalcanti

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Março/2002

João Pessoa - Pb

Cripto-Sistemas com Chave Pública Baseado em Extensões Cúbicas

por

Almir César Ferreira Cavalcanti

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva - UFPB (Orientador)

Prof. Dr. Hélio Pires de Almeida - UFPB

Prof. Dr. Martinho da Costa Araújo - UFMT

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Março/2002

Agradecimentos

1. Ao Professor Dr. *Antônio de Andrade e Silva*, que compreende o verdadeiro sentido da palavra *orientação*.

2. Ao amigo Andrade, pela paciência, dedicação, compreensão e amizade.

3. Aos professores Hélio Pires de Almeida, Marivaldo Pereira Matos, João Marcos Bezerra do Ó e Roberto Callejas Bedregal que muito contribuiram para a minha formação.

4. Ao Adelmo, pelo carinho e companheirismo.

5. Aos colegas do curso de mestrado, em especial aos amigos Geraldo Lúcio Tardin, Paulo Roberto Lemos de Messias, Cícero José da Silva, Claudilene Gomes da Costa e Walter Chagas de Morais

6. A Sônia, pela competência e presteza no atendimento de secretaria.

7. Aos colegas do Departamento de Matemática - UFMT - Campus de Rondonópolis.

8. A Professora Olga Nakajima do Departamento de Matemática - UFMT.

9. Aos amigos de sempre: Tati, Joselma, Lau, Kida, Flávio, Rosa, Júlio, Wilse e Maristela pelo carinho e incentivo.

10. Ao amigo JB que apresentou o verde e a musicalidade da cidade.

Dedicatória

Aos meus pais
Almerindo e Hilda , e
aos meus irmãos Léo, Paulo,
Dida, Beibe e Ana Paula. A
famíla que ama e sabe amar.

Resumo

As propriedades criptográficas de uma seqüência recursiva linear de terceira ordem sobre um corpo finito $\mathbb{F}_p$ são investigadas. Um primeiro algoritmo computacional para calcular o k-ésimo termo de uma seqüência característica de ordem 3 é apresentado. Baseando-se nessas propriedades, um novo sistema de distribuição de chave pública e um algoritmo de codificação do tipo-RSA são propostos.

Abstract

The cryptographic properties of third-order linear feedback shift-register sequences over $\mathbb{F}_p$ are investigated. A fast computational algorithm for evaluating the kth term of a characteristic sequence of order 3 is presented. Based on these properties, a new public-key distribution scheme and an RSA-type encryption algorithm are proposed.

Notação

G - Grupo

aH - Classe lateral à esqueda de H em G

$\frac{G}{H}$ - Grupo quociente de G por H

$\langle g \rangle$ - Subgrupo cíclico de G gerado por g

$\mathbb{Z}_n$ - Anel dos inteiros módulo n

$\mathbb{Z}_n^\bullet$ - Grupo multiplicativo dos elementos inversíveis de $\mathbb{Z}_n$

$\text{mdc}(a, b)$ - Máximo divisor comum de a e b

$\varphi(n)$ - Função de Euler

$\mathbf{M}_2(\mathbb{Z}_n)$ - Conjunto das 2×2 matrizes invertíveis sobre o anel $(\mathbb{Z}_n)$

$\mathbb{F}_p$ - Corpo de Galois de ordem p

$\mathbb{F}^\bullet$ - Grupo cíclico multiplicativo do corpo $\mathbb{F}$

$\mathbb{F}_p[x]$ - Anel dos polinômios sobre o corpo $\mathbb{F}_p$

$(\frac{a}{p})$ - Símbolo de Legendre

$\partial(f)$ - Grau do polinômio f

$f^\perp$ - Polinômio recíproco de f

$[L : K]$ - Grau de L sobre K

$\mathbf{s}$ - Seqüência

$per(\mathbf{s})$ - Período da seqüência $\mathbf{s}$

$\mathbb{N}$ - Conjunto dos números naturais

$\mathbb{Z}$ - Conjunto dos números inteiros

$\equiv$ - Congruente

$|$ - Divide

$\cong$ - Isomorfo

$\forall$ - Para todo

$\sum$ - Soma

$\mathbb{A}$ - Alfabeto

$\mathcal{P}$ - Conjunto de todas as possíveis mensagens unitárias $\mathbf{u}$

$\mathcal{C}$ - Conjunto de todas as possíveis mensagens unitárias $\mathbf{c}$

k_c - Chave de codificação

k_d - Chave de decodificação

$\mathbf{A}$ - Matriz

Γ - Função lógica

Sumário

.

Introdução

Criptografia é a arte ou ciência de escrever mensagens em cifra ou em código, de modo que somente a pessoa autorizada possa decifrar e ler as mensagens.

A mensagem a ser enviada é chamada de *texto-original* (plaintext) e a mensagem codificada é chamada de *texto-cifrado* (ciphertext). O texto-original e o texto-cifrado são escritos em algum alfabeto $\mathbb{A}$ consistindo de um certo número n de símbolos; isto é,

$$\#(\mathbb{A}) = n.$$

O processo de converter um texto-original para um texto-cifrado é chamado de *codificação* ou *cifragem*, e o processo de reverter é chamado de *decodificação* ou *decifragem*.

O *processo de codificação* é uma função que associa cada mensagem unitária $\mathbf{u}$ do texto-original a uma mensagem unitária $\mathbf{c}$ do texto-cifrado. Mais precisamente, sejam $\mathcal{P}$ o conjunto de todas as possíveis mensagens unitárias $\mathbf{u}$ do texto-original e $\mathcal{C}$ o conjunto de todas as possíveis mensagens unitárias $\mathbf{c}$ do texto-cifrado. Então a correspondência biunívoca

$$f : \mathcal{P} \to \mathcal{C} \text{ tal que } f(\mathbf{u}) = \mathbf{c}$$

é o processo de codificação. A correspondência biunívoca

$$f^{-1} : \mathcal{C} \to \mathcal{P} \text{ tal que } f^{-1}(\mathbf{c}) = \mathbf{u}$$

é o processo de decodificação. Assim, temos o seguinte diagrama

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

Cripto-sistema

Um *Cripo-sistema* é qualquer bijeção de $\mathcal{P}$ sobre $\mathcal{C}$.

Com o rápido desenvolvimento de aplicações na internet, informações seguras no mundo de hoje são mais importantes do que em épocas passadas. Projetos de cripto-

sistemas que alcancem requerimentos de faixa de comunicação, taxa de informação, velocidade computacional, e estratégias de segurança têm se tornado um grande desafio para os pesquisadores.

Uma grande parte dos pesquisadores usam cripto-sistemas modernos tais como o RSA (Rivest, Shamir e Adleman), sistemas criptográficos com chave pública DH (Diffie e Hellman), cripto-sistema ElGamal e DSS (Digital Signature Standard), aumentando o comprimento do módulo para fortalecer sua segurança.

Do ponto de vista das seqüências recursivas lineares, a função exponencial utilizada na codificação do sistema RSA, do sistema criptográfico com chave pública DH e do sistema de assinatura digital ElGamal é uma seqüência recursiva linear de ordem 1 sobre $\mathbb{F}_q$ ou $\mathbb{Z}_n$, onde n é um produto de dois números primos. Na literatura, existem outras famílias de cripto-sistemas similares ao RSA, ao DH e ao cripto-sistema com chave pública ElGamal, que são chamadas de *sistema polinomial Dickson*. A função matemática utilizada nessas famílias de cripto-sistemas com chave pública é a seqüência recursiva linear de ordem 2 sobre $\mathbb{F}_q$ ou $\mathbb{Z}_n$ com valores iniciais especiais. Estas espécies de seqüência recursiva linear são classes constantes.

Nesta dissertação, estudamos cripto-sistemas com chave pública, isto é, cripto-sistemas onde codificação e decodificação são governados por chaves distintas: k_c é a chave de codificação (pública) e k_d é a chave de decodificação (secreta), de modo que calcular k_d a partir de k_c é computacionalmente impraticável, necessitando de 10^{100} instruções. Esses cripto-sistemas possuem uma estrutura assimétrica, em outras palavras, a função codificadora $f : \mathcal{P} \to \mathcal{C}$ é fácil de calcular quando a chave de codificação k_c é conhecida, mas na prática é muito difícil calcular a função inversa $f^{-1} : \mathcal{C} \to \mathcal{P}$, isto é, do ponto de vista da realidade computacional, a função f não é inversível (para calcular f^{-1} se faz necessário uma informação adicioanal - a chave de decodificação k_d). Tal função f é chanada de "*trapdoor function*".

Estudamos cripto-sistema com chave pública utilizando uma seqüência recursiva linear de ordem 3 sobre $\mathbb{F}_q$ ou $\mathbb{Z}_n$, isto é, uma seqüência $s_0, s_1, \ldots$ de elementos em $\mathbb{F}_q$ tais que

$$s_{n+3} = a_2 s_{n+2} + a_1 s_{n+1} + a_0 s_n,$$

para todo inteiro n maior que ou igual a zero, com a_0, a_1 e a_2 em $\mathbb{F}_q$.

No primeiro capítulo apresentamos alguns resultados básicos da teoria dos grupos, dos anéis e das seqüências recursivas lineares homogêneas, necessários para uma melhor com-

preensão do texto. Investigamos algumas propriedades criptográficas de uma seqüência recursiva linear de ordem 3 e mostramos um rápido algoritmo computacional proposto por Guang Gong e Lein Harn em [6] para calcular o k-ésimo termo de uma seqüência característica de ordem 3, isto é, uma seqüência gerada por um polinômio característico

$$f(x) = x^3 - ax^2 + bx - 1$$

pertencente a $\mathbb{F}_q[x]$, com a e b em $\mathbb{F}_q$, tal que, os elememtos da seqüência satisfaçam a relação de recorrência

$$s_k = as_{k-1} - bs_{k-2} + s_{k-3}$$

para k maior que ou igual a 3, com valores iniciais $s_0 = 3$, $s_1 = a$ e $s_2 = a^2 - 2b$.

Baseando-se nessas propriedades estudamos dois algoritmos criptográficos propostos por Guang Gong e Lein Harn em [6]. O primeiro é um sistema de distribuição com chave pública GH-PKD que pode reduzir o comprimento do módulo e aumentar a velocidade computacional. A segurança deste sistema baseia-se na dificuldade de solucionar logaritmos discretos em $\mathbb{F}_{p^3}$. O segundo é um algoritmo de codificação do tipo-RSA cuja segurança baseia-se na dificuldade de fatorar um grande número inteiro composto, em um produto de dois primos

No segundo capítulo mostramos alguns sistemas clássicos de criptografia; o sistema de distribuição DH, que intoduziu o conceito de criptografia com chave pública proposto por Diffie e Hellman em 1976, utilizando um sistema de parâmetros público: um número primo estremamente grande p (com aproximadamente 100 dígitos) e t um elemento primitivo módulo p, isto é, o mdc$(t, p) = 1$; e concluímos o mesmo com a demonstração do sistema de distribuição com chave pública GH-PKD,

$$\left[\begin{array}{ccc} u_i \text{ calcula} & \overset{(s_{r_i}, s_{-r_i})}{\rightarrow} & u_j \text{ calcula} \\ \\ s_{r_i}\left(s_{r_j}, s_{-r_j}\right) \text{ e } s_{-r_i}\left(s_{r_j}, s_{-r_j}\right) & \overset{(s_{r_j}, s_{-r_j})}{\leftarrow} & s_{r_j}\left(s_{r_i}, s_{-r_i}\right) \text{ e } s_{-r_j}\left(s_{r_i}, s_{-r_i}\right) \end{array}\right]$$

proposto por Guag e Harn, construído através de um par se seqüências características de ordem 3, com um sistema de parâmetros público: um número primo p e um polinômio

$$f(x) = x^3 - ax^2 + bx - 1$$

irredutível sobre $\mathbb{F}_p$.

No terceiro e último capítulo apresentamos o sistema de criptografia com chave pública RSA, proposto por Rivest, Shamir e Adleman. O aspecto crucial deste sistema é que n é o produto de dois grandes números primos de valores aproximadamente iguais e que fatorar números inteiros grandes se constitui em um problema impraticável. Nesse sistema, a mensagem a ser codificada é dividida em blocos e cada bloco considerado como um inteiro entre 0 e $n-1$. O sistema baseia-se no fato que é praticamente impossível encontrar k_d tal que

$$k_c \cdot k_d \equiv 1 \,(\mathrm{mod}\, n),$$

sem conhecer a fatoração de n; esta é uma generalização do teorema de Fermat. Para finalizar, mostramos também um cripto-sistema com chave pública do tipo-RSA, proposto por Guag e Harn em [6], usando um par de seqüências características sobre $\mathbb{Z}_n$.

Nesta dissertação, discutimos apenas o funcionamento dos algorítmos. Não nos detemos às questões de segurança, implementação e custos dos algoritmos estudados.

Capítulo 1

Resultados Básicos

Neste capítulo apresentaremos alguns resultados básicos dos números inteiros, da teoria dos grupos, anéis e seqüência recursiva linear que serão necessários nos capítulos seguintes.

1.1 Inteiros

Nesta seção apresentaremos alguns resultados da teoria dos número que serão necessários para a compreensão desta dissertação. O leitor interessado em mais detalhes deve consultar [14].

Um dos axiomas que será usado implicitamente muitas vezes, é o seguinte:

Axioma 1.1 (Boa Ordenação) *Todo subconjunto não vazio de* $\mathbb{N}$ *contém um menor elemento.*

Teorema 1.1 (Princípio de Indução 1ª Forma) *Seja* X *um subconjunto de* $\mathbb{N}$ *com as seguintes propriedades*:

1. $1 \in X$;

2. $\forall k \in \mathbb{N}$, $k \in X \Rightarrow k+1 \in X$. *Então* $X = \mathbb{N}$. ■

Teorema 1.2 (Princípio de Indução 2ª Forma) *Seja* X *um subconjunto de* $\mathbb{N}$ *com as seguintes propriedades*:

1. $1 \in X$;

2. $\forall k \in \mathbb{N}$, $\{1, 2, \ldots, k\} \subseteq X \Rightarrow k+1 \in X$. *Então* $X = \mathbb{N}$. ■

Teorema 1.3 (Algoritmo da Divisão) *Sejam $a, b \in \mathbb{Z}$ com $b > 0$. Então existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = qb + r, \quad onde \ 0 \leq r < b.$$

■

1.2 Grupos

Nesta seção apresentaremos alguns resultados clássicos da teoria dos grupos que serão necessários para a compreensão desta dissertação. O leitor interessado em mais detalhes pode consultar [1, 4].

Um conjunto não vazio G equipado com uma operação binária

$$\begin{aligned} * : \ & G \times G \longrightarrow G \\ & (a, b) \longmapsto a * b \end{aligned}$$

é um *grupo* se as seguintes condições são satisfeitas:

1. $a * (b * c) = (a * b) * c$, para todos $a, b, c \in G$.

2. Existe $e \in G$ tal que $e * a = a * e = a$, para todo $a \in G$.

3. Para todo $a \in G$, existe $b \in G$ tal que $a * b = b * a = e$.

O grupo é *abeliano* ou *comutativo* se também vale a condição

4. $a * b = b * a$, para todos $a, b \in G$.

Com o objetivo de simplificar a notação usaremos ab em vez $a * b$. A *ordem* ou *cardinalidade* de um grupo G é o número de elementos de G e denotaremos por $|G|$.

Sejam G um grupo e H um subconjunto de G. Dizemos que H é um *subgrupo* de G, em símbolos $H \leq G$, se as seguintes condições são satisfeitas:

1. $H \neq \emptyset$;

2. $ab^{-1} \in H$, para todos $a, b \in H$.

Sejam G um grupo e H um subgrupo de G. Dado $a \in G$, o conjunto

$$aH = \{ah : \forall h \in H\}$$

é chamado a *classe lateral à esquerda* de H em G determinada por a. De modo semelhante, podemos definir a classe lateral à direita Ha de H em G. O conjunto de todas as classes laterais à esquerda de H em G formam uma partição de G, que denotamos por $\frac{G}{H}$.

Dados $a, b \in G$, dizemos que a *é congruente a* b *módulo* H se $a^{-1}b \in H$, que denotamos por $a \equiv b \pmod{H}$. É fácil verificar que $\equiv$ é uma relação de equivalência em G e que a classe de equivalência determinada por a é igual a classe lateral à esquerda aH. O elemento a é chamado um *representante* da classe de equivalência. É também fácil verificar que existe uma correspondência biunívoca entre o conjunto das classes laterais à esquerda de H em G e o conjunto das classes laterais à direita de H em G. A cardinalidade do conjunto das classes laterais à esquerda (ou à direita) de H em G é chamado o *índice* de H em G, que denotamos por $(G : H)$.

Sejam G um grupo e H um subgrupo de G. Dizemos que H é um *subgrupo normal* de G, em símbolos $H \trianglelefteq G$, se

$$Ha = aH, \forall a \in G,$$

isto é,

$$aHa^{-1} = H, \forall a \in G.$$

Sejam G um grupo e H um subgrupo de G. Então $\frac{G}{H}$ é um grupo com operação $aHbH = abH$, para todos $a, b \in G$, se, e somente se, H é um subgrupo normal de G. Neste caso, $\frac{G}{H}$ é chamado o *grupo quociente* de G por H.

Teorema 1.4 (Lagrange) *Sejam G um grupo finito e H um subgrupo de G. Então $|H|$ divide $|G|$.* ■

Sejam $g \in G$ e

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

Então é claro que $\langle g \rangle$ é um subgrupo de G chamado de *subgrupo cíclico* de G gerado por g. Um grupo G é dito *cíclico* se existir $g \in G$ tal que $G = \langle g \rangle$. A ordem de um elemento $g \in G$, em símbolos $o(g)$, é definida como $o(g) = |\langle g \rangle|$. É fácil verificar que se $o(g)$ é finita, então $o(g)$ é igual ao menor inteiro positivo k tal que $g^k = e$.

Exemplo 1.1 *Seja $n \in \mathbb{N}$ fixado, definimos no conjunto*

$$\begin{aligned} \mathbb{Z}_n &= \{\overline{a} : a \in \mathbb{Z}\} \\ &= \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}, \end{aligned}$$

onde

$$\begin{aligned} \overline{a} &= \{m \in \mathbb{Z} : m \equiv a \,(\mathrm{mod}\, n)\} \\ &= \{a + kn : k \in \mathbb{Z}\}, \end{aligned}$$

duas operações binária

$$\overline{a} \oplus \overline{b} = \overline{a+b} \;\; e \;\; \overline{a} \odot \overline{b} = \overline{ab}.$$

É fácil verificar que estas operações são bem definidas e que $(\mathbb{Z}_n, \oplus)$ é um grupo cíclico gerado por $\overline{1}$. Além disso,

$$\begin{aligned} (\mathbb{Z}_n, \odot) &= \{\overline{a} \in \mathbb{Z}_n : \overline{a} \odot \overline{x} = \overline{x} \odot \overline{a} = \overline{1}, \;\; \textit{para algum } \overline{x} \in \mathbb{Z}_n\} \\ &= U(\mathbb{Z}_n) \end{aligned}$$

é um grupo, chamado grupo multiplicativo dos elementos inversíveis de $\mathbb{Z}_n$.

Teorema 1.5 *Seja G um grupo cíclico. Então todo subgrupo de G é cíclico.*

Prova. Seja $G = \langle a \rangle$ e $H \leq G$. Se $H = \{1\}$, então $H = \langle 1 \rangle$. Suponhamos que $H \neq \{1\}$. Então existe $m \in \mathbb{Z}$ tal que $a^m, a^{-m} \in H$ com $m \neq 0$. Logo, o conjunto

$$S = \{n \in \mathbb{N} : a^n \in H\}$$

é não vazio. Assim, pelo Princípio da Boa Ordenação, S contém um menor elemento, digamos k.

Afirmação. $H = \langle a^k \rangle$.

De fato, é claro que $\langle a^k \rangle \subseteq H$. Por outro lado, dado $y \in H$, existe $m \in \mathbb{Z}$ tal que $y = a^m$. Aplicando o Algoritmo da Divisão a m e k, obtemos que

$$m = qk + r, \;\; \text{onde } 0 \leq r < k.$$

Se $r > 0$, então

$$a^r = a^{m-qk} = (a^m)(a^k)^{-q} \in H$$

com $r < k$, o que é uma contradição. Logo, $r = 0$ e

$$y = a^m = (a^k)^q \in \langle a^k \rangle .$$

Portanto, $H \subseteq \langle a^k \rangle$. ■

Teorema 1.6 *Seja G um grupo. Então:*

1. *Se $a \in G$ tem ordem n, então $a^m = 1$ se, e somente se, $n \mid m$.*
2. *Se $G = \langle a \rangle$ tem ordem n, então $G = \langle a^k \rangle$ se, e somente se,* $\text{mdc}\,(k, n) = 1$.
3. *Se $a \in G$ tem ordem n, então $n = |\langle a \rangle|$.*

Prova. 1. Aplicando o Algoritmo da Divisão a m e n, obtemos que

$$m = qn + r, \text{ onde } 0 \leq r < n.$$

Se $r > 0$, então

$$a^r = a^{m-qn} = a^m (a^n)^{-q} = 1,$$

o que contradiz a minimalidade de n. Logo $r = 0$ e $n \mid m$. Reciprocamente, se $m = nk$, então

$$a^m = a^{nk} = (a^n)^k = 1^k = 1.$$

2. Suponhamos que $G = \langle a^k \rangle$. Como $a \in G$ temos que existem $t \in \mathbb{Z}$ tal que $a = a^{tk}$. Logo,

$$a^{tk-1} = a^{tk} a^{-1} = aa^{-1} = 1.$$

Assim, pelo item 1., $n \mid (tk - 1)$, isto é, existe $s \in \mathbb{Z}$ tal que

$$tk - 1 = sn.$$

Logo, $\text{mdc}\,(k, n) = 1$.

Reciprocamente, se $\text{mdc}\,(k, n) = 1$, então existem $r, s \in \mathbb{Z}$ tais que

$$rk + sn = 1.$$

Logo,

$$a = a^1 = a^{rk+sn} = \left(a^k\right)^r (a^n)^s = \left(a^k\right)^r \in \langle a^k \rangle .$$

Portanto, $G = \langle a^k \rangle$.

3. Os elementos

$$1, a, \ldots, a^{n-1}$$

são todos distintos, pois se existissem $0 \leq i < j < n$ tais que $a^j = a^i$, então, $a^{j-i} = 1$ com $i - j < n$, o que contradíz a minimalidade de n. É claro que

$$\left\{1, a, \ldots, a^{n-1}\right\} \subseteq \langle a \rangle .$$

Reciprocamente, dado $y \in \langle a \rangle$, existe $m \in \mathbb{Z}$ tal que $y = a^m$. Aplicando o Algoritmo da Divisão a m e n, obtemos que

$$m = qn + r, \text{ onde } 0 \leq r < n.$$

Se $r > 0$, então

$$y = a^m = a^{qn+r} = (a^n)^q a^r = a^r \in \left\{1, a, \cdots, a^{n-1}\right\} .$$

Logo,

$$\langle a \rangle \subseteq \left\{1, a, \ldots, a^{n-1}\right\} .$$

Portanto, $n = |\langle a \rangle|$. ■

Lema 1.1 *Se $G = \langle a \rangle$ tem ordem n, então G contém um único subgrupo de ordem d para cada $d \mid n$.*

Prova. Seja $n = kd$. Então $H = \left\langle a^k \right\rangle$ tem ordem d. De fato, seja $r = |H|$. Então

$$a^{kr} = (a^k)^r = 1.$$

Logo,

$$n \mid kr \Rightarrow kd \mid kr \Rightarrow d \mid r \Rightarrow d \leq r.$$

Por outro lado,

$$1 = a^n = a^{kd} = \left(a^k\right)^d \Rightarrow r \mid d \Rightarrow r \leq d.$$

Portanto, $r = d$. Finalmente, seja K um subgrupo de G de ordem d. Então $K = \langle a^m \rangle$. Logo,

$$1 = a^{md} \Rightarrow n \mid md \Rightarrow kd \mid md \Rightarrow k \mid m.$$

Assim, existe $r \in \mathbb{Z}$ tal que $m = kr$. Logo,

$$a^m = a^{kr} = (a^k)^r \in H \Rightarrow K \subseteq H.$$

Portanto, $H = K$. ■

A função $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ dada por

$$\varphi(n) = |\{m : 1 \leq m \leq n \text{ e } \operatorname{mdc}(n, m) = 1\}|$$

é chamada de *função de Euler*. Por exemplo,

$$\varphi(6) = 2.$$

Observação 1.1 *Se*

$$g(G) = \{a \in G : a \text{ é um gerador de } G\},$$

então $|g(G)| = \varphi(n)$.

Teorema 1.7 *Se* $n \in \mathbb{N}$, *então* $n = \sum_{d|n} \varphi(d)$.

Prova. Seja G um grupo cíclico de ordem n. Pelo Lema 1.1, para cada divisor d de n existe um único subgrupo cíclico H_d de G de ordem d. Logo,

$$|g(H_d)| = \varphi(d).$$

Como cada elemento de G gera exatamente um dos subgrupos H_d temos que

$$G = \dot{\bigcup_{d|n}} g(H_d).$$

Assim,

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

■

Teorema 1.8 *Seja* G *um grupo de ordem* n. *Então* G *é cíclico se, e somente se, para cada divisor* d *de* n *existe no máximo um subgrupo cíclico de ordem* d.

Prova. Pelo Lema 1.1, basta provar a recíproca. Para cada $d \mid n$, seja $\lambda(d)$ o número de elementos de ordem d em G. Como cada elemento de G tem a ordem unicamente determinada por $d \mid n$ temos que

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

Afirmação. $\lambda(d) \leq \varphi(d)$.

De fato, se $\lambda(d) \geq 1$, então existe $a \in G$ tal que $a^d = 1$. Como cada $a^k \in G$, com $1 \leq k \leq d$ e $\text{mdc}(k, d) = 1$, tem ordem d temos que existem pelo menos $\varphi(d)$ elementos de ordem d. Assim,

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

Desde que $\lambda(d) \leq \varphi(d)$ para todo d, obtemos que $\lambda(d) = \varphi(d)$ para todo $d \mid n$. Em particular, $\lambda(n) = \varphi(n) \geq 1$. Portanto, G contém um subgrupo cíclico de ordem n, isto é, G é cíclico. ■

Teorema 1.9 (Euler) *Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então*

$$a^{\varphi(n)} \equiv 1 \,(\text{mod}\, n).$$

Prova. Como $\text{mdc}(a, n) = 1$ temos que $\overline{a}$ é um elemento do grupo multiplicativo $\mathbb{Z}_n^\bullet$. Pelo Teorema de Lagrange, $\overline{a}^{\varphi(n)} = \overline{1}$, pois $|\mathbb{Z}_n^\bullet| = \varphi(n)$. Portanto,

$$a^{\varphi(n)} \equiv 1 \,(\text{mod}\, n).$$

■

Corolário 1.1 (Fermat) *Seja $p \in \mathbb{N}$ um número primo. Então*

$$a^p \equiv a \,(\text{mod}\, p), \forall a \in \mathbb{Z}.$$

■

Observação 1.2 *O Teorema de Euler pode ser usado para determinar o inverso de todo elemento $\overline{a} \in \mathbb{Z}_n^\bullet$, pois*

$$a^{\varphi(n)} \equiv 1 \,(\text{mod}\, n) \Leftrightarrow a^{-1} \equiv a^{\varphi(n)-1} \,(\text{mod}\, n).$$

1.3 Anéis

Nesta seção apresentaremos alguns resultados clássicos da teoria de anéis que serão necessários para a compreensão desta dissertação. O leitor interessado em mais detalhes pode consultar [1, 4].

Um *anel* é um conjunto não vazio R equipado com duas operações binárias, adição $(x, y) \to x + y$ e multiplicação $(x, y) \to xy$, tal que as seguintes propriedades valem:

1. R é um grupo comutativo sob a adição.

2. $x(yz) = (xy)z$, para todos $x, y, z \in R$.

3. $x(y+z) = xy + xz$, $(x+y)z = xz + yz$, para todos $x, y, z \in R$.

   Se um anel R satisfaz as propriedades:

4. Existe $1 \in R$ tal que $x1 = 1x = x$, para todo $x \in R$, dizemos que R é um *anel com identidade.*

5. $xy = yx$, para quaisquer $x, y \in R$, dizemos que R é um *anel comutativo*

   Se um anel R satisfaz a propriedade:

6. Para todos $x, y \in R$, $xy = 0 \Rightarrow x = 0$ ou $y = 0$, dizemos que R é um *anel sem divisores de zero.* Caso contrário, dizemos que R é um *anel com divisores de zero.*

Dizemos que um elemento $x \in R$, $x \neq 0$, é *regular* se x não é divisor de zero.

Se R é um anel comutativo, com identidade e sem divisores de zero, dizemos que R é um *domínio.* Um elemento $x \in R$ é dito uma *unidade* de R se existir $y \in R$ tal que $xy = yx = 1$. Denotaremos por $U(R)$ o conjunto de todas as unidades de R. Se

$$U(R) = R^* = R - \{0\},$$

dizemos que R é um *corpo.*

Exemplo 1.2 *O anel $\mathbb{Z}_n$ é um corpo se, e somente se, n é um número primo.*

Se R é um anel, então existe um inteiro positivo n tal que $nr = 0$ para todo $r \in R$. O menor n tal que $nr = 0$ é chamado de característica do anel R.

Um subconjunto não vazio S de um anel R é um *subanel* de R se as seguintes condições são satisfeitas:

1. para todos $x, y \in S$, tem-se $x + y \in S$;

2. para todos $x, y \in S$, tem-se $xy \in S$;

3. $1 \in S$.

Um subconjunto não vazio I de um anel R é um *ideal* de R se as seguintes condições são satisfeitas:

1. para todos $x, y \in I$, tem-se $x - y \in I$;

2. Para todo $x \in I$ e $r \in R$, tem-se $rx \in I$.

Um ideal I do anel R tal que $I \neq 0$ e $I \neq R$ é chanado *ideal próprio.*

Sejam R e S dois anéis. Uma função $\phi : R \longrightarrow S$ é um *homomorfismo de anéis* se as seguintes condições são satisfeitas:

1. $\phi(x + y) = \phi(x) + \phi(y)$, para todos $x, y \in R$;

2. $\phi(xy) = \phi(x)\phi(y)$, para todos $x, y \in R$.

Um homomorfismo de anéis $\phi : R \longrightarrow S$ é um *isomorfismo* se ϕ é bijetiva. Quando existir um isomorfismo entre R e S dizemos que R e S são *isomorfos* e denotaremos por $R \cong S$.

Teorema 1.10 *Sejam R, S dois anéis e $\phi : R \longrightarrow S$ um homomorfismo de anéis. Então*

$$\frac{G}{\ker \phi} \cong \operatorname{Im} \phi.$$

■

Teorema 1.11 *Sejam $n_1, \ldots, n_k \in \mathbb{N}$ tais que $n_i \geq 2$ e $\operatorname{mdc}(n_i, n_j) = 1$, se $i \neq j$. Então*

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k},$$

onde $n = n_1 \cdots n_k$.

Prova. Vamos definir a função

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \text{ por } \phi(a) = (a \,(\operatorname{mod} n_1), \ldots, a \,(\operatorname{mod} n_k)).$$

É claro que ϕ é bem definida e um homomorfismo de anéis. Assim,

$$\frac{\mathbb{Z}}{\ker \phi} \cong \operatorname{Im} \phi \text{ e } \ker \phi = n_1\mathbb{Z} \cap \cdots \cap n_k\mathbb{Z} = n\mathbb{Z}.$$

Agora, vamos provar que ϕ é sobrejetora. Dado

$$(b_1 \,(\operatorname{mod} n_1), \ldots, b_k \,(\operatorname{mod} n_k)) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}.$$

É claro que

$$\frac{n}{n_i} \in \mathbb{Z} \text{ e } \operatorname{mdc}(\frac{n}{n_i}, n_i) = 1,$$

para todo $i = 1, 2, \ldots, k$. Logo, para cada i existe $x_i \in \mathbb{Z}$ tal que

$$\frac{n}{n_i}x_i \equiv 1 \,(\mathrm{mod}\, n_i) \text{ e } \frac{n}{n_i}x_i b_i \equiv b_i \,(\mathrm{mod}\, n_i).$$

Se $j \neq i$, então é fácil verificar que

$$\frac{n}{n_i}x_i \equiv 0 \,(\mathrm{mod}\, n_j) \text{ e } \frac{n}{n_i}x_i b_i \equiv 0 \,(\mathrm{mod}\, n_j).$$

Assim, existe

$$a = \sum_{i=1}^{k} \frac{n}{n_i}x_i b_i \in \mathbb{Z}$$

tal que

$$\phi(a) = (b_1 \,(\mathrm{mod}\, n_1), \ldots, b_k \,(\mathrm{mod}\, n_k)).$$

Logo, ϕ é sobrejetora. Portanto,

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k},$$

onde $n = n_1 \cdots n_k$. ■

Observação 1.3 (Teorema Chinês dos Restos) *O fato de que ϕ é sobrejetora, Teorema 1.11, significa que dados $b_1, \ldots, b_k \in \mathbb{Z}$, existe $x \in \mathbb{Z}$ tal que*

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, n_1) \\ x \equiv b_2 \,(\mathrm{mod}\, n_2) \\ \quad \vdots \\ x \equiv b_k \,(\mathrm{mod}\, n_k) \end{cases}.$$

Um ideal não nulo M de um anel R é um *ideal maximal* de R se $M \neq R$ e se J é um ideal de R tal que $M \subseteq J \subseteq R$, então $M = J$ ou $J = R$.

Proposição 1.1 *Seja I um ideal próprio de R. Então I é maximal se, e somente se, $\langle I, r\rangle = R$, para todo $r \in R - I$.* ■

Teorema 1.12 *Sejam R um anel e M um ideal de R. Então M é maximal se, e somente se, $\frac{R}{M}$ é um corpo.* ■

Denotaremos por $M_2(\mathbb{Z}_n)$ o conjunto das 2×2 matrizes com entradas sobre o anel $\mathbb{Z}_n$.

Teorema 1.13 *Sejam*

$$A = \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} \in M_2(\mathbb{Z}_n) \ \ e \ \ D = ad - bc \in \mathbb{Z}.$$

Então as seguintes condições são equivalentes:

1. $\text{mdc}(n, D) = 1$;

2. *A tem uma matriz inversa*;

3. *A função*

$$T : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n \ \ \textit{dada por} \ T\left(\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}\right) = A \begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}$$

   é uma correspondência biunívoca;

4. *Se* $\overline{x}$ *ou* $\overline{y} \in \mathbb{Z}_n^*$, *então*

$$T\left(\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}\right) \neq \begin{bmatrix} \overline{0} \\ \overline{0} \end{bmatrix}.$$

Prova. (*1.* $\Rightarrow$ *2.*) Suponhamos que $\text{mdc}(n, D) = 1$. Então existe $\overline{D}^{-1} \in \mathbb{Z}_n$ tal que

$$\overline{D} \odot \overline{D}^{-1} = \overline{1}.$$

Portanto,

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

é a matriz inversa de A. É fácil verificar que (*2.* $\Rightarrow$ *3.*) e (*3.* $\Rightarrow$ *4.*). Assim, resta mostrar que (*4.* $\Rightarrow$ *1.*), Suponhamos que $\text{mdc}(n, D) = k > 1$ e seja $n = km$. Então há três casos a serem considerados:

(i) Se todas as entradas de A são divisíveis por k, então pondo

$$\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix} = \begin{bmatrix} \overline{m} \\ \overline{m} \end{bmatrix}, \ \text{obtemos que} \ T\left(\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}\right) = \begin{bmatrix} \overline{0} \\ \overline{0} \end{bmatrix}.$$

(ii) Se a e b não são ambos divisíveis por k, então pondo

$$\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix} = \begin{bmatrix} -\overline{bm} \\ \overline{am} \end{bmatrix}, \ \text{obtemos que} \ T\left(\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}\right) = \begin{bmatrix} \overline{0} \\ \overline{0} \end{bmatrix},$$

pois n divide Dm.

(iii) Se c e d não são divisíveis por k, então pondo

$$\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix} = \begin{bmatrix} \overline{dm} \\ -\overline{cm} \end{bmatrix}, \text{ obtemos que } T\left(\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}\right) = \begin{bmatrix} \overline{0} \\ \overline{0} \end{bmatrix},$$

pois n divide Dm. ■

Lema 1.2 *Sejam $a, n \in \mathbb{N}$, com $\text{mdc}(a, n) = 1$. Se $r, t \in \mathbb{N}$ são tais que $rt \equiv 1 \pmod{\varphi(n)}$, então*

$$a^{rt} \equiv a \pmod{n}.$$

Prova. Como $rt \equiv 1 \pmod{\varphi(n)}$ temos que existe $s \in \mathbb{N}$ tal que

$$rt = 1 + s\varphi(n).$$

Logo,

$$a^{rt} = a^{1+s\varphi(n)} = a \cdot a^{s\varphi(n))} = a\left(a^{\varphi(n)}\right)^s \equiv a \cdot 1^s \equiv a \pmod{n}.$$

■

Corolário 1.2 *Sejam $n, r, t \in \mathbb{N}$. Se $\text{mdc}(t, \varphi(n)) = 1$, então a função*

$$f : \mathbb{Z}_n \to \mathbb{Z}_n \text{ dada por } f(\overline{x}) = \overline{x}^t$$

é uma correspondência biunívoca com $f^{-1}(\overline{x}) = \overline{x}^r$, onde $rt \equiv 1 \pmod{\varphi(n)}$. ■

Sejam $p \in \mathbb{N}$ um número primo e

$$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$$

um conjunto de inteiros. Então $\phi : \mathbb{Z}_p \to \mathbb{F}_p$ definida por $\phi(\overline{a}) = a$ é uma bijeção. Logo, $\mathbb{F}_p$ com as operações induzidas por ϕ é um corpo finito, chamado de *corpo de Galois* de ordem p. Portanto, ϕ é um isomorfismo.

Sejam $\mathbb{F}$ um corpo finito e $\mathbb{K}$ um subcorpo de $\mathbb{F}$, então o grau de $\mathbb{F}$ sobre $\mathbb{K}$, em símbolos $[\mathbb{F} : \mathbb{K}]$, é a dimensão de $\mathbb{F}$ visto como um espaço vetorial sobre $\mathbb{K}$. O corpo $\mathbb{F}$ é chamado uma extensão finita de $\mathbb{K}$ se $[\mathbb{F} : \mathbb{K}]$ é finito.

Lema 1.3 *Sejam $\mathbb{F}$ um corpo finito e $\mathbb{K}$ um subcorpo de $\mathbb{F}$ com $|\mathbb{K}| = q$. Então $|\mathbb{F}| = q^m$, onde $[\mathbb{F} : \mathbb{K}] = m$.*

Prova. Como $\mathbb{F}$ é um espaço vetorial sobre $\mathbb{K}$ e $\mathbb{F}$ é finito temos que $[\mathbb{F} : \mathbb{K}] = m$, para algum $m \in \mathbb{N}$. Assim,

$$\mathbb{F} \cong \mathbb{K}^m.$$

Portanto, $|\mathbb{F}| = q^m$. ■

Corolário 1.3 *Seja $\mathbb{F}$ um corpo finito. Então $|\mathbb{F}| = p^m$, onde p é a característica de $\mathbb{F}$ e $[\mathbb{F} : \mathbb{Z}_p] = m$.* ■

Note que, pelo Teorema de Fermat temos que $a^q = a$, para todo a pertecente a um corpo finito $\mathbb{F}$, com q elementos.

Teorema 1.14 *Se $\mathbb{F}$ é um corpo finito, então $\mathbb{F}^\bullet$ é cíclico e $\mathbb{F} = \mathbb{Z}_p(\alpha)$, para algum α.*

Prova. Suponhamos que $|\mathbb{F}^\bullet| = n$ e $d \mid n$. Seja H um subgrupo cíclico de $\mathbb{F}^\bullet$ com ordem d. Então, pelo Teorema de Lagrange, $x^d = 1, \forall x \in H$. Suponhamos, por absurdo, que $\mathbb{F}^\bullet$ contenha um outro subgrupo cíclico K com ordem d. Então existe pelo menos um $b \in K$ tal que $b \notin H$. Assim, $\mathbb{F}^\bullet$ contém pelo menos $d+1$ elementos tais que $y^d = 1$, o que é uma cantradição, pois $x^d - 1$ contém no máximo d raízes em $\mathbb{F}^\bullet$. Logo, $\mathbb{F}^\bullet$ contém no máximo um subgrupo cíclico de ordem d. Portanto, $\mathbb{F}^\bullet$ é cíclico. ■

Seja $\mathbb{F}$ um corpo finito de característica p. Dizemos que $\alpha \in \mathbb{F}$ é um *elemento primitivo* se $\mathbb{F} = \mathbb{Z}_p(\alpha)$.

Dizemos que $a \in \mathbb{F}$ é um *quadrado* se existir $u \in \mathbb{F}$ tal que $u^2 = a$. Quando existir $u \in \mathbb{F}$ tal que $u^2 = a$, dizemos que a é um *resíduo quadrático módulo p*; caso contrário, dizemos que a é um *resíduo não quadrático.*

Teorema 1.15 *Seja a um inteiro não divisível por um primo p. Então*:

1. $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$;

2. *a é resíduo quadrático módulo p se, e somente se,*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p};$$

3. *a é resíduo não quadrático módulo p se, e somente se,*

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

■

Seja $\text{mdc}(a,p)=1$. Definimos o *símbolo de Legendre* por

$$\left(\frac{a}{p}\right)=\begin{cases} 1 & \text{se } a \text{ é resíduo quadrático módulo } p \\ -1 & \text{se } a \text{ é resíduo não quadrático módulo } p \end{cases}.$$

Pode ser mostrado que

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Corolário 1.4 *Seja $\mathbb{F}$ um corpo finito de característica p. Se $a,b\in\mathbb{F}$ são não quadrados, então ab é um quadrado.* ■

Seja R um anel. Um elemento $p\in R^*$ é *irredutível* sobre R se as seguintes condições são satisfeitas:

1. $p\notin U(R)$;
2. Se $p=bc$, então $b\in U(R)$ ou $c\in U(R)$, isto é, p não tem divisores próprios.

Sejam R um anel e

$$R^{seq}=\{f=(a_i)_{i\in\mathbb{Z}_+}:a_i\in R\}$$

o conjunto das *seqüências formais* sobre R tais que $a_i\neq 0$ somente para um número finito de índices. Dados $f=(a_i)_{i\in\mathbb{Z}_+}, g=(b_i)_{i\in\mathbb{Z}_+}\in R^{seq}$, dizemos que

$$f=g\Leftrightarrow a_i=b_i,\forall i\in\mathbb{Z}_+.$$

Definimos em R^{seq} duas operações binárias, adição e multiplicação, por

$$f+g=(a_0+b_0,a_1+b_1,\ldots)\ \text{ e }\ fg=(c_0,c_1,\ldots),$$

onde

$$c_k=\sum_{i+j=k}a_ib_j.$$

Note que, somente um número finito de termos aparece nesta soma, pois se $i+j=k$, então $0\leq i,j\leq k$. Com estas operações R^{seq} é um anel comutativo com identidade, o qual será chamado de *anel dos polinômios* na variável x.

Seja

$$S=\{(a,0,0,\ldots):a\in R\}.$$

Então, S é um subanel de R^{seq} isomorfo a R. Assim, podemos identificar

$$(a, 0, 0, \ldots) \text{ com } a.$$

Vamos denotar o símbolo ax por

$$(0, a, 0, \ldots).$$

Mais geralmente, o símbolo ax^n denota

$$(0, 0, \ldots, 0, a, 0, \ldots),$$

onde a está na $(n+1)$-ésima posição. Usando essa notação, cada seqüência

$$f = (a_0, a_1, \ldots, a_n, 0, \ldots)$$

pode ser escrita de modo único na forma

$$\begin{aligned} f &= (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + \cdots + (0, \ldots, 0, a_n, 0, \ldots) + \cdots \\ &= a_0 + a_1 x + \cdots + a_n x^n \\ &= \sum_{i=0}^{n} a_i x^i. \end{aligned}$$

Para identificar a indeterminada x vamos denotar R^{seq} por $R[x]$.

Podemos escrever $F[x]$ para indicar o conjunto dos polinômios na variável x sobre o corpo F.

Quando

$$f = a_0 + a_1 x + \cdots + a_n x^n \in F[x] \text{ e } b \in F,$$

para $x = b$, obtemos

$$f = a_0 + a_1 b + \cdots + a_n b^n$$

o qual é um elemento de F.

Assim, em qualquer identidade polinomial em $F[x]$ podemos substituir um elemento fixado $b \in F$ por x e obter uma identidade válida em F. Dizemos que um elemento $b \in F$ é uma raiz do polinômio $f \in F[x]$ se $f(b) = 0$.

Proposição 1.2 *Seja $f \in F[x]$. Então f é irredutível sobre o corpo F se, e somente se,*

$$\frac{F[x]}{\langle f \rangle}$$

é um corpo. ■

Se $F = \mathbb{F}_p$ e $\partial(f) = m$, então o número de elementos do corpo

$$\frac{F[x]}{\langle f \rangle} = \{r + \langle f \rangle : r \in F[x] \text{ e } \partial(r) < m\}$$

é igual ao número de polinômios em $F[x]$ com grau menor do que m, a saber, p^m. Neste caso,

$$\frac{F[x]}{\langle f \rangle} \cong \mathbb{F}_{p^m}$$

Teorema 1.16 (Kronecker) *Se $f \in K[x]$ é irredutível sobre o corpo K, então existe um corpo L contendo K e as raízes de f.* ■

Seja $f \in F[x]$ irredutível sobre o corpo F. Então, pelo Teorema de Kronecker, existe um corpo L, contendo F tal que

1. $f = (x - a_1) \cdots (x - a_m)$ em L;
2. $L = F[a_1, \ldots, a_m]$.

O corpo L é chamado o *corpo de decomposição* de f sobre F.

Teorema 1.17 *Seja f um polinômio irredutível sobre $\mathbb{F}_q$ de grau k. Então f divide $x^{q^n} - x$ se, e somente se, k divide n.*

Prova. Suponhamos que f divide $x^{q^n} - x$. Seja α uma raiz de f em um corpo de decomposição de f sobre $\mathbb{F}_q$. Então $\alpha^{q^n} = \alpha$. Logo, $\alpha \in \mathbb{F}_{q^n}$. Assim, $\mathbb{F}_q[\alpha]$ é um subcorpo de $\mathbb{F}_{q^n}$. Como $[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = k$ e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ temos que

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q[\alpha]] \cdot [\mathbb{F}_q[\alpha] : \mathbb{F}_q]] = k \cdot [\mathbb{F}_{q^n} : \mathbb{F}_q[\alpha]],$$

isto é, k divide n. Reciprocamente, suponhamos que k divide n. Então $q^k - 1$ divide $q^n - 1$. Logo, $\mathbb{F}_{q^k} \subseteq \mathbb{F}_{q^n}$. Seja α uma raiz de f em um corpo de decomposição de f sobre $\mathbb{F}_q$. Então $[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = k$ e $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^k}$, logo $\alpha \in \mathbb{F}_{q^n}$ e $\alpha^{q^n} = \alpha$, isto é, α é uma raiz de $x^{q^n} - x$. Portanto, f divide $x^{q^n} - x$. ■

Seja α uma raíz de um polinômio irredutível $f \in \mathbb{F}_q$ de grau k, onde $q = p^r$ e p a característica de $\mathbb{F}_q$. Então,

$$\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{k-1}}$$

são todas as outras raízes de f, chamadas *conjugadas* de α. Como $\mathrm{mdc}(p, q-1) = 1$ temos que

$$\left(\alpha^{q^j}\right)^{q-1} = 1,$$

pois $\mathbb{F}_q^{\bullet}$ é um grupo cíclico de ordem $q-1$.

Lema 1.4 *Seja $f \in \mathbb{F}_q[x]$ um polinômio de grau $m \geq 1$ com $f(0) \neq 0$. Então existe um inteiro positivo $e \leq q^m - 1$ tal que f divide $x^e - 1$.*

Prova. Como

$$\frac{\mathbb{F}_q[x]}{\langle f \rangle}$$

possui $q^m - 1$ classes não nulas, temos que

$$x^j + \langle f \rangle, 0 \leq j \leq q^m - 1$$

são todas não nulas. Logo, existem inteiros s e t com $0 \leq s < t \leq q^m - 1$ tais que

$$x^t \equiv x^s \pmod{f}.$$

Desde que $\mathrm{mdc}(x, f) = 1$, obtemos

$$f \mid (x^{t-s} - 1) \text{ e } 0 < t - s \leq q^m - 1.$$

■

Seja $f \in \mathbb{F}_q[x]$ um polinômio não nulo. Se $f(0) \neq 0$, então o menor $e \in \mathbb{N}$ tal que

$$f \mid (x^e - 1)$$

é chamado a *ordem* de f. Se $f(0) = 0$, então f é da forma $x^l g$, para algum $l \in \mathbb{N}$ e um único polinômio $g \in \mathbb{F}_q[x]$ com $g(0) \neq 0$. Neste caso, a ordem de f é definida como a ordem de g.

Teorema 1.18 *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau $m \geq 2$. Então a ordem de f é igual a ordem de alguma raíz de f em $\mathbb{F}_q^{\bullet}$.*

Prova. Como $\mathbb{F}_{q^m}$ é o corpo de decomposição de f sobre $\mathbb{F}_q$ temos que as raízes de f tem a mesma ordem em $\mathbb{F}_{q^m}^{\bullet}$. Seja $\alpha \in \mathbb{F}_{q^m}^{\bullet}$ uma raíz de f. Então $\alpha^e = 1$ se, e somente se, $f \mid x^e - 1$. Sendo f irredutível e $m \geq 2$, obtemos que $f(0) \neq 0$. Portanto, pela definição, a ordem de f é igual a ordem de α em $\mathbb{F}_{q^m}^{\bullet}$. ■

Corolário 1.5 *Se $f \in \mathbb{F}_q[x]$ é irredutível sobre $\mathbb{F}_q$ tem grau m, então a ordem de f divide $q^m - 1$.* ■

Um polinômio mônico irredutível de grau m sobre $\mathbb{F}_q$ é chamado *primitivo* se ele é o polinômio minimal de um elemento primitivo de $\mathbb{F}_{q^m}$.

Teorema 1.19 *Um polinômio $f \in \mathbb{F}_q[x]$ de grau m é primitivo se, e somente se, f é mônico, $f(0) \neq 0$ e a ordem de f é igual a $q^m - 1$.*

Prova. Se f é primitivo sobre sobre $\mathbb{F}_q$, então f é mônico e $f(0) \neq 0$. Como f é irredutível sobre $\mathbb{F}_q$ temos, pelo Teorema 1.18, que a ordem de f é igual a $q^m - 1$. Reciprocamente, basta mostrar que f é irredutível. Suponhamos, por absurdo, que f é redutível. Então há dois casos a serem considerados:

1º Caso. Se $f = gh$, onde $1 \leq \partial(g), \partial(h) < \partial(f)$. Sejam $m_1 = \partial(g)$, $m_2 = \partial(h)$, e_1 e e_2 as ordens de g e h, respectivamente. Então a ordem e de f é tal que $e \leq e_1 e_2$. Como

$$g \mid x^{q^{m_1}-1} - 1 \text{ e } g \mid x^{q^{m_2}-1} - 1$$

temos que $e_i \leq q^{m_i} - 1$. Logo,

$$e \leq e_1 e_2 \leq (q^{m_1} - 1)(q^{m_2} - 1) < q^m - 1,$$

o que é uma contradição.

2º Caso. Se $f = g^r$, onde $r \in \mathbb{N}$, $g(0) \neq 0$ e g é irredutível. Seja e a ordem de g. Então $e \mid q^m - 1$, pois $g \mid f$. Assim, $\text{mdc}(e, p) = 1$, onde p é a característica de $\mathbb{F}_q$. Logo, se $e \mid k$, então $g \mid x^k - 1$. Assim, se $k = p^i b$, onde $\text{mdc}(b, p) = 1$, então

$$x^k - 1 = (x^b - 1)^{p^i}.$$

Como $x^b - 1$ não tem raízes repetidas temos que todos os fatores irredutíveis de $x^b - 1$ têm a mesma multiplicidade p^i. Seja t o único inteiro tal que

$$p^{t-1} < r \leq p^t.$$

Então a ordem de f é igual a ep^t. Mas

$$ep^t \leq (q^n - 1)p^t < q^{n+t} - 1,$$

onde $n = \frac{m}{r} = \partial(g)$. Assim,

$$t \leq p^{t-1} \leq r - 1 \leq (r-1)n.$$

Logo, a ordem de f

$$ep^t < q^{n+t} - 1 \leq q^{rn} - 1 = q^m - 1,$$

o que é uma contradição. ■

Corolário 1.6 *Seja*

$$\mathbb{F}_{q^m} = \frac{\mathbb{F}_q[x]}{\langle f \rangle},$$

onde a ordem de f é igual $q^m - 1$. Então $\alpha = x + \langle f \rangle$ é um elemento primitivo em $\mathbb{F}_{q^m}$, assim

$$\mathbb{F}_{q^m} = \left\{0, 1, \alpha, \alpha^2, \cdots, \alpha^{q^m-2}\right\}.$$

■

1.4 Seqüência Recursiva Linear

Nesta seção trataremos apenas das seqüências recursivas lineares homogêneas de ordem 3, o leitor interessado em mais detalhes pode consultar [8, 9].

Uma seqüência $s_0, s_1, \ldots$ de elementos em $\mathbb{F}_q$ é uma *seqüencia recursiva linear de ordem* 3 em $\mathbb{F}_q$, se existirem elementos $a_0, a_1, a_2 \in \mathbb{F}_q$ tais que

$$s_{n+3} = a_2 s_{n+2} + a_1 s_{n+1} + a_0 s_n, \forall n = 0, 1, \ldots \tag{1.1}$$

Os termos s_0, s_1, s_2 da seqüência são chamados *valores iniciais* e a equação 1.1 é chamada uma *relação de recorrência linear de odem* 3.

O vetor $\mathbf{s}_n = (s_n, s_{n+1}, s_{n+2})$ é chamado o n-ésimo *vetor de estado* e $\mathbf{s}_0 = (s_0, s_1, s_2)$ é chamado o *vetor de estado inicial*.

Sejam $\mathbb{S}$ um conjunto arbitrário e $s_0, s_1, \ldots$ uma seqüência em $\mathbb{S}$. A seqüência é chamada de *maior período* se existirem $r, n_0 \in \mathbb{N}$ tais que $s_{n+r} = s_n$, para todo $n \geq n_0$. O número n_0 é chamado de *pré-período* e o número r é chamado o *período* da seqüência. O menor de todos os possíveis períodos de uma seqüência de maior período é chamado de *menor período*. Uma das características das seqüências recursivas lineares em $\mathbb{F}_q$ é que elas são periódicas.

Lema 1.5 *Seja $s_0, s_1, \ldots$ uma seqüência recursiva linear de ordem 3 de maior período em $\mathbb{F}_q$. Então todo período é divisível pelo menor período.*

Prova. Sejam r o período e s o menor período. Então existem $n_1, n_2 \in \mathbb{N}$ tais que $s_{n+r} = s_n$, para todo $n \geq n_1$ e $s_{n+s} = s_n$, para todo $n \geq n_2$. Suponhamos, por absurdo, que s não divide r. Então, pelo Algoritmo da Divisão, existem únicos $q, t \in \mathbb{N}$ tais que

$$r = qs + t, \text{ onde } 0 < t < s.$$

Tomando $n_0 \geq \max\{n_1, n_2\}$, obtemos que

$$\begin{aligned} s_n &= s_{n+r} \\ &= s_{n+qs+t} \\ &= s_{n+t}, \end{aligned}$$

o que é uma contradição, pois $t < s$. ■

Uma seqüência de maior período com menor período r é chamada *periódica* se

$$s_{n+r} = s_n, \forall n = 0, 1, \ldots$$

Lema 1.6 *A seqüência $s_0, s_1, \ldots$ é periódica se, e somente se, existir um inteiro $r > 0$ tal que $s_{n+r} = s_n$, para todo $n = 0, 1, \ldots$*

Prova. Suponhamos que a seqüência $s_0, s_1, \ldots$ é periódica. Então existe um $r > 0$ tal que $s_{n+r} = s_n$, para todo $n = 0, 1, \ldots$. Reciprocamente, suponhamos que exista um inteiro $r > 0$ tal que $s_{n+r} = s_n$, para todo $n = 0, 1, \ldots$. Então a seqüência é de maior período com menor período s. Assim, existe $n_0 \in \mathbb{N}$ tal que $s_{n+s} = s_n$, para todo $n \geq n_0$. Seja $n \in \mathbb{Z}_+$ qualquer e escolhemos $m \geq n_0$ com $m \equiv n \pmod{r}$. Então

$$\begin{aligned} s_{n+s} &= s_{m+s} \\ &= s_m \\ &= s_n. \end{aligned}$$

Portanto, a seqüência é periódica. ■

Teorema 1.20 *Toda seqüência recursiva linear $s_0, s_1, \ldots$ de ordem 3 em $\mathbb{F}_q$ é de maior período com menor período $r \leq q^3 - 1$.*

Prova. Suponhamos que o vetor estado inicial $\mathbf{s}_t = (s_t, s_{t+1}, s_{t+2}) \neq \mathbf{0}$ (caso contrário, $\mathbf{s}_{t+1} = \mathbf{s}_{t+2} = \cdots = \mathbf{0}$). Como $|(\mathbb{F}_{q^3})^*| = q^3 - 1$ temos que para os vetores de estados $\mathbf{s}_m$, $0 \leq m \leq q^3 - 1$, em uma seqüência recursiva linear $s_0, s_1, \ldots$ de ordem 3 em $\mathbb{F}_q$, deve existir i e j com $0 \leq i < j \leq q^3 - 1$ tais que $\mathbf{s}_i = \mathbf{s}_j$. Usando as relações de recursão linear e indução, obtemos $\mathbf{s}_{n+j-i} = \mathbf{s}_n$ para todo $n \geq i$. Portanto, $s_0, s_1, \ldots$ é uma seqüência de maior período com menor período $0 \leq r \leq j - i \leq q^3 - 1$. ■

Teorema 1.21 *Se $s_0, s_1, \ldots$ é uma seqüência recursiva linear em $\mathbb{F}_q$ satisfazendo* 1.1 *com $a_0 \neq 0$, então a seqüência é periódica.*

Prova. Pelo Teorema 1.20, temos que a seqüência recursiva linear em $\mathbb{F}_q$ é de maior período. Se r é o menor período e n_0 é o pré-período, então $s_{n+r} = s_n$, para todo $n \geq n_0$. Suponhamos, por absurdo, que $n_0 \geq 1$. Então

$$\begin{aligned} s_{n_0-1+r} &= a_0^{-1}(s_{n_0+r+2} - a_2 s_{n_0+r+1} - a_1 s_{n_0+r}) \\ &= a_0^{-1}(s_{n_0+2} - a_2 s_{n_0+1} - a_1 s_{n_0}). \end{aligned}$$

Usando 1.1 com $n = n_0 - 1$, achamos a mesma expressão para s_{n_0-1}. Assim,

$$s_{n_0-1+r} = s_{n_0-1},$$

o que é uma contradição, pois $n_0 - 1 < n_0$. ■

Exemplo 1.3 *Seja $s_0, s_1, \ldots$ uma seqüência recursiva linear de ordem* 3 *em $\mathbb{F}_5$ com $s_0 =$ 3, $s_1 = 4$, $s_2 = 1$ e*

$$s_{n+3} = -s_{n+2} + s_n, \forall n = 0, 1, \ldots$$

Então por inspeção, obtemos que

$$s_{n+24} = s_n, \forall n = 0, 1, \ldots$$

Note que, o menor período 24 *da seqüência recursiva linear não divide $5^3 - 1 = 124$.*

Podemos associar a seqüência recursiva linear de ordem 3 em $\mathbb{F}_q$, satisfazendo a Equação 1.1, a 3×3 matriz

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & a_0 \\ 1 & 0 & a_1 \\ 0 & 1 & a_2 \end{bmatrix}.$$

A matriz $\mathbf{A}$ é chamada de *matriz companheira* da seqüência recursiva linear de ordem 3.

Teorema 1.22 *Sejam $s_0, s_1, \ldots$ uma seqüência recursiva linear de ordem 3 em $\mathbb{F}_q$ satisfazendo* 1.1 *e* $\mathbf{A}$ *sua matriz companheira. Então o vetor da seqüência satisfaz*

$$\mathbf{s}_n = \mathbf{s}_0\mathbf{A}^n, \forall n = 0, 1, \ldots$$

Prova. Seja $\mathbf{s}_0 = (s_0, s_1, s_2)$ o vetor de estado inicial. Então

$$\begin{aligned}
\mathbf{s}_1 &= (s_1, s_2, s_3) \\
&= (s_1, s_2, a_2s_2 + a_1s_1 + a_0s_0) \\
&= s_0(0, 0, a_0) + s_1(1, 0, a_1) + s_2(0, 1, a_2) \\
&= \mathbf{s}_0\mathbf{A}.
\end{aligned}$$

De modo análogo, mostra-se que

$$\mathbf{s}_2 = \mathbf{s}_1\mathbf{A} = (\mathbf{s}_0\mathbf{A})\mathbf{A} = \mathbf{s}_0\mathbf{A}^2.$$

Portanto, por indução, obtemos o resultado. ■

Teorema 1.23 *Seja $s_0, s_1, \ldots$ uma seqüência recursiva linear homogênea de ordem 3 em $\mathbb{F}_q$ com $a_0 \neq 0$. Então o período da seqüência é um divisor da ordem da matriz companheira $\mathbf{A}$ no grupo $GL(3, \mathbb{F}_q)$ das matrizes 3×3 invertíveis sobre $\mathbb{F}_q$.*

Prova. Como $\det \mathbf{A} = -a_0 \neq 0$ temos que $\mathbf{A} \in GL(3, \mathbb{F}_q)$. Assim, se m é a ordem de $\mathbf{A}$ em $GL(3, \mathbb{F}_q)$, então

$$\begin{aligned}
\mathbf{s}_{n+m} &= \mathbf{s}_0\mathbf{A}^{n+m} \\
&= \mathbf{s}_0\mathbf{A}^n \\
&= \mathbf{s}_n, \forall n = 0, 1, \ldots
\end{aligned}$$

Portanto, m é um período da seqüência. ■

Seja $s_0, s_1, \ldots$ uma seqüência recursiva linear homogênea de ordem 3 em $\mathbb{F}_q$. Então o polinômio

$$f = x^3 - a_2x^2 - a_1x - a_0 \in \mathbb{F}_q[x]$$

é chamado o *polinômio característico* da seqüência.

O polinômio

$$f^{\perp} = -x^3 f(\frac{1}{x}) = -1 + a_2x + a_1x^2 + a_0x^3 \in \mathbb{F}_q[x]$$

é o *polinômio característico recíproco*. Note que, a ordem de f é igual a ordem $f^{\perp}$.

Lema 1.7 *Para o polinômio mônico f, a matriz companheira $\mathbf{A}$ tem polinômio minimal f.*

Prova. Seja $\mathbf{T} : \mathbb{F}_p^3 \to \mathbb{F}_p^3$ o operador linear que é representado em relação à base canônica de $\mathbb{F}_p^3$ pela matriz

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & a_0 \\ 1 & 0 & a_1 \\ 0 & 1 & a_2 \end{bmatrix}.$$

Então, $\mathbf{T}(e_1) = e_2, \mathbf{T}(e_2) = e_3$, e $\mathbf{T}(e_3) = a_0e_1 + a_1e_2 + a_2e_3$. Assim,

$$\left\{e_1, \mathbf{T}(e_1), \mathbf{T}^2(e_1)\right\}$$

é uma base de $\mathbb{F}_p^3$. Logo, para cada $\alpha \in \mathbb{F}_p^3$ existem únicos $c_1, c_2, c_3 \in \mathbb{F}_p$ tais que

$$\begin{aligned} \alpha &= c_1e_1 + c_2\mathbf{T}(e_1) + c_3\mathbf{T}^2(e_1) \\ &= g(\mathbf{T})(e_1) \end{aligned}$$

onde g é um polinômio de grau no máximo igual a 2. Além disso,

$$\mathbf{T}^3(e_1) = a_0e_1 + a_1e_2 + a_2e_3,$$

de modo que $f(\mathbf{T})(e_1) = 0$. Portanto,

$$f(\mathbf{T})(\alpha) = 0,$$

isto é, f também é o polinômio minimal, pois

$$g(\mathbf{T})(e_1) = \alpha \neq 0$$

para todo polinômio g de grau menor do que ou igual a 2. ■

Lema 1.8 *Seja $s_0, s_1, \ldots$ uma seqüência recursiva linear homogênea de ordem 3 em $\mathbb{F}_q$ com polinômio característico $f \in \mathbb{F}_q[x]$. Então o período da seqüência é um divisor da ordem de f.*

Prova. Pelo Lema 1.7

$$f = \det(x\mathbf{I} - \mathbf{A})$$

é o polinômio minimal de $\mathbf{A}$. Assim, $\mathbf{A}^e = \mathbf{I}$, para algum $e \in \mathbb{N}$ se, e somente se, $f \mid x^e - 1$. Portanto, o período da seqüência é um divisor da ordem de f. ■

Corolário 1.7 *Seja $s_0, s_1, \ldots$ uma seqüência recursiva linear homogênea de ordem 3 em $\mathbb{F}_q$ com polinômio característico $f \in \mathbb{F}_q[x]$. Então o menor período da seqüência é um divisor da ordem de f. Se $f(0) \neq 0$, então ela é periódica.* ■

Teorema 1.24 *Sejam $s_0, s_1, \ldots$ uma seqüência recursiva linear de ordem 3 em $\mathbb{F}_q$ satisfazendo 1.1 com período r e f seu polinômio característico. Então*

$$f \cdot s = (1 - x^r)h$$

com

$$s = s_0 x^{r-1} + \cdots + s_{r-2}x + s_{r-1} \in \mathbb{F}_q[x]$$

e

$$h = \sum_{j=0}^{2} \sum_{i=0}^{2-j} a_{i+j+1} s_i x^j \in \mathbb{F}_q[x],$$

onde tomamos $a_3 = -1$. ■

Teorema 1.25 *Sejam $s_0, s_1, \ldots$ uma seqüência recursiva linear de ordem 3 em $\mathbb{F}_q$ satisfazendo 1.1 com vetor estado inicial não nulo e f seu polinômio característico. Se f é irredutível sobre $\mathbb{F}_q$ e $f(0) \neq 0$, então a seqüencia é periódica com menor período igual a ordem de f.*

Prova. Pelo Corolário 1.7 a seqüencia é periódica e seu menor período r divide a ordem de f, isto é, r é menor ou igual a ordem de f. Por outro lado, pelo Teorema 1.24, $f(x)$ divide $(x^r - 1)\, h(x)$, como $s \neq 0$ temos que $h \neq 0$. Ora, sendo f irredutível e $\partial(h) < \partial(f)$, obtemos que f divide $(x^r - 1)$. Portanto, a ordem de f é menor que ou igual a r. ■

Agora vamos restringir o estudo de seqüência à seqüência recursiva linear homogênea de ordem 3 em $\mathbb{F}_p$

$$s_k = as_{k-1} - bs_{k-2} + s_{k-3}, \forall k = 3, 4, \ldots \tag{1.2}$$

com polinômio característico

$$f = x^3 - ax^2 + bx - 1, a, b \in \mathbb{F}_p.$$

e valores iniciais

$$s_0 = 3, s_1 = a \text{ e } s_2 = a^2 - 2b.$$

Denotaremos s_k por $s_k(a, b)$ ou $s_k(f)$ e $\mathbf{s}$ como $s(a, b)$ ou $s(f)$.

Suponhamos que α_1, α_2 e α_3 sejam as raízes de f no corpo de decomposição de f sobre $\mathbb{F}_p$. Então

$$\begin{aligned} \alpha_1+\alpha_2+\alpha_3 &= a \\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= b \\ \alpha_1\alpha_2\alpha_3 &= 1. \end{aligned}$$

Como

$$\begin{aligned} \alpha_1^3 &= a\alpha_1^2-b\alpha_1+1 \\ \alpha_2^3 &= a\alpha_2^2-b\alpha_2+1 \\ \alpha_3^3 &= a\alpha_3^2-b\alpha_3+1 \end{aligned}$$

temos que

$$\begin{aligned} \alpha_1^{n+3}+\alpha_2^{n+3}+\alpha_3^{n+3} &= a(\alpha_1^{n+2}+\alpha_2^{n+2}+\alpha_3^{n+2})-b(\alpha_1^{n+1}+\alpha_2^{n+1}+\alpha_3^{n+1}) \\ &\quad +(\alpha_1^n+\alpha_2^n+\alpha_3^n), \end{aligned}$$

para todo $n\in\mathbb{Z}_+$. Portanto,

$$s_k(a,b)=\alpha_1^k+\alpha_2^k+\alpha_3^k, \forall k=3,4,\ldots \tag{1.3}$$

Como $\alpha_1\alpha_2=\alpha_3^{-1}$, $\alpha_1\alpha_3=\alpha_2^{-1}$ e $\alpha_2\alpha_3=\alpha_1^{-1}$ temos que

$$\begin{aligned} s_{-1} &= \alpha_1^{-1}+\alpha_2^{-1}+\alpha_3^{-1}=b, \\ s_{-2} &= b^2-2a. \end{aligned}$$

Logo, temos a seqüência recursiva linear homogênea de ordem 3 em $\mathbb{F}_p$

$$s_{-k}=bs_{-k+1}-as_{-k+2}+s_{-k+3}, \forall k=3,4,\ldots$$

com polinômio característico

$$f^{\perp}=x^3-bx^2+ax-1.$$

Portanto,

$$\begin{aligned} s_{-k}(a,b) &= \alpha_1^{-k}+\alpha_2^{-k}+\alpha_3^{-k} \\ &= s_k(b,a), \forall k=3,4,\ldots \end{aligned}$$

Lema 1.9 *Sejam $s_0, s_1, \ldots$ uma seqüência recursiva linear de ordem 3 em $\mathbb{F}_p$ satisfazendo* 1.2*, f seu polinômio característico, $\alpha_1, \alpha_2, \alpha_3$ suas raízes e*

$$f_k = (x - \alpha_1^k)(x - \alpha_2^k)(x - \alpha_3^k). \tag{1.4}$$

Então:

1. $f_k = x^3 - s_k(a,b)\,x^2 + s_{-k}(a,b)\,x - 1$, *onde* $s_{-k}(a,b) = s_k(b,a)$;
2. f *e* f_k *têm a mesma ordem e se, e somente se,* $\mathrm{mdc}(e,k) = 1$;
3. *Se* $\mathrm{mdc}(e,k) = 1$, *então f é irredutível sobre $\mathbb{F}_p$ se, e somente se, f_k é irredutível sobre $\mathbb{F}_p$.*

Prova. 1. Como

$$(\alpha_1\alpha_2)^n = \alpha_3^{-n}, (\alpha_1\alpha_3)^n = \alpha_2^{-n} \text{ e } (\alpha_2\alpha_3)^n = \alpha_1^{-n}, \forall n \in \mathbb{N}$$

temos, pela equação 1.3, que

$$\begin{aligned} s_{-k}(a,b) &= \alpha_1^{-k} + \alpha_2^{-k} + \alpha_3^{-k} \\ &= \alpha_2^k\alpha_3^k + \alpha_1^k\alpha_3^k + \alpha_1^k\alpha_2^k \\ &= s_k(b,a). \end{aligned}$$

Portanto,

$$f_k = x^3 - s_k(a,b)\,x^2 + s_{-k}(a,b)\,x - 1.$$

2. Pela prova do Lema 1.8, temos que o polinômio minimal de α_i^k e α_i tem a mesma ordem e se, e somente se, $\mathrm{mdc}(e,k) = 1$.

3. É uma conseqüência de 2. ■

Lema 1.10 *Sejam $s_0, s_1, \ldots$ uma seqüência recursiva linear de ordem 3 em $\mathbb{F}_p$ satisfazendo* 1.2*, f seu polinômio característico e $\alpha_1, \alpha_2, \alpha_3$ suas raízes. Então*

$$s_k(s_l(a,b), s_{-l}(a,b)) = s_{kl}(a,b), \forall k, l \in \mathbb{Z}_+.$$

Prova. Pelo Lema 1.9, temos que

$$\begin{aligned} f_l &= \left(x - \alpha_1^l\right)\left(x - \alpha_2^l\right)\left(x - \alpha_3^l\right) \\ &= x^3 - s_l(a,b)\,x^2 + s_{-l}(a,b)\,x - 1. \end{aligned}$$

Portanto,

$$\begin{aligned} s_k(s_l(a,b), s_{-l}(a,b)) &= \left(\alpha_1^l\right)^k + \left(\alpha_2^l\right)^k + \left(\alpha_3^l\right)^k \\ &= \alpha_1^{lk} + \alpha_2^{lk} + \alpha_3^{lk} \\ &= s_{kl}(a,b). \end{aligned}$$

■

Fato 1.1 *Como $s_k(a,b)$ e $s_{-k}(a,b)$ são polinômios ortogonais em $\mathbb{F}_p[a,b]$ temos, pelo Teorema [9, Theorem, 7.46, p.377], que o sistema de equações*

$$s_k(a,b) = u \ \text{ e } \ s_{-k}(a,b) = v,$$

para algum $u, v \in \mathbb{F}_p$, tem uma única solução $(a,b) \in \mathbb{F}_p \times \mathbb{F}_p$ se, e somente se,

$$\text{mdc}(k, p^i - 1) = 1, i = 1, 2, 3$$

Denotaremos por

$$Q = p^2 + p + 1,$$

a ordem de um polinômio irredutível sobre $\mathbb{F}_p$.

Um inteiro positivo k é chamado um líder de classe módulo Q se k é o menor inteiro no conjunto

$$\{lp^i \pmod{Q} : i = 0, 1, 2 \text{ e } l \in \mathbb{Z}_+\}.$$

onde l é um inteiro positivo.

Teorema 1.26 *Sejam $f = x^3 - ax^2 + bx - 1$ um polinômio irredutível sobre $\mathbb{F}_p$ de ordem $Q = p^2 + p + 1$ e $s(f)$ uma seqüência associada a f. Sejam k e k' diferentes líderes de classe módulo Q, com $\text{mdc}(k, Q) = \text{mdc}(k', Q) = 1$. Então*

$$(s_k, s_{-k}) \neq (s_{k'}, s_{-k'}).$$

Prova. Suponhamos, por absurdo, que

$$(s_k, s_{-k}) = (s_{k'}, s_{-k'}).$$

Então

$$\begin{aligned} f_k &= x^3 - s_k x^2 + s_{-k} x - 1 \\ &= x^3 - s_{k'} x^2 + s_{-k'} x - 1 \\ &= f_{k'}. \end{aligned}$$

Assim, $\alpha_i^{k'}$, $1 \leq i \leq 3$, são raízes de f_k. Como, pelo Lema 1.9, f_k é irredutível sobre $\mathbb{F}_p$ temos que α_i^k e $\alpha_i^{k'}$ são conjugadas uma da outra. Logo, existe inteiro t, $0 \leq t \leq 2$, tal que

$$k' \equiv kp^t \pmod{Q},$$

o que é uma contradição, pois k e k' são diferentes líderes de classe módulo Q. ■

Lema 1.11 *Sejam $s_0, s_1, \ldots$ uma seqüência recursiva linear de ordem 3 em $\mathbb{F}_q$ satisfazendo 1.2, f seu polinômio característico, $\alpha_1, \alpha_2, \alpha_3$ suas raízes e $s_0, s_{-1}, \ldots$ sua seqüência recíproca. Então:*

1. $s_{2n} = s_n^2 - 2s_{-n}, \forall m, n \in \mathbb{Z}_+$;

2. $s_n s_m - s_{n-m} s_{-m} = s_{n+m} - s_{n-2m}, \forall m, n \in \mathbb{Z}_+$ *com* $n \neq m$.

Prova. 1. Pela equação 1.3, obtemos que

$$s_{2n} = \alpha_1^{2n} + \alpha_2^{2n} + \alpha_3^{2n} \text{ e } s_n^2 = \left(\alpha_1^n + \alpha_2^n + \alpha_3^n\right)^2.$$

Como $\alpha_1 \alpha_2 \alpha_3 = 1$ temos que

$$\begin{aligned} s_n^2 &= \alpha_1^{2n} + \alpha_2^{2n} + \alpha_3^{2n} + 2 \sum_{1 \leq i < j \leq 3} \alpha_i^n \alpha_j^n \\ &= s_{2n} + 2 \sum_{i=1}^{3} \alpha_i^{-n} \\ &= s_{2n} + 2s_{-n} \end{aligned}$$

2. Pela equação 1.3, obtemos que

$$\begin{aligned} s_n &= \alpha_1^n + \alpha_2^n + \alpha_3^n \\ s_{n+m} &= \alpha_1^{n+m} + \alpha_2^{n+m} + \alpha_3^{n+m} \\ s_{n-m} &= \alpha_1^{n-m} + \alpha_2^{n-m} + \alpha_3^{n-m} \\ s_{-m} &= \alpha_1^{-m} + \alpha_2^{-m} + \alpha_3^{-m} \\ s_{n-2m} &= \alpha_1^{n-2m} + \alpha_2^{n-2m} + \alpha_3^{n-2m}. \end{aligned}$$

Assim,

$$\begin{aligned} s_n s_m &= (\alpha_1^n + \alpha_2^n + \alpha_3^n) \cdot (\alpha_1^m + \alpha_2^m + \alpha_3^m) \\ &= s_{n+m} + \sum_{i=1}^{3} \sum_{j=1}^{3} \alpha_i^n \alpha_j^m, i \neq j, \end{aligned}$$

e

$$\begin{aligned} s_{n-m} s_{-m} &= \left(\alpha_1^{n-m} + \alpha_2^{n-m} + \alpha_3^{n-m}\right) \cdot \left(\alpha_1^{-m} + \alpha_2^{-m} + \alpha_3^{-m}\right) \\ &= s_{n-2m} + \sum_{i=1}^{3} \sum_{j=1}^{3} \alpha_i^n \alpha_j^m, i \neq j, \end{aligned}$$

pois $\alpha_1 \alpha_2 \alpha_3 = 1$. Portanto,

$$s_n s_m - s_{n-m} s_{-m} = s_{n+m} - s_{n-2m}.$$

■

Capítulo 2

Criptografia

Neste capítulo apresentaremos o sistema de criptografia com chave pública DH e um sistema de distribuição com chave-pública (GH-PKD), que é construído por um par de seqüências características de ordem 3. Não trataremos aqui dos problemas de segurança, complexidade, etc.

2.1 Cripto-sistemas

Nesta seção apresentaremos alguns resultados básicos sobre sistemas clássicos de criptografia. O leitor interessado em mais detalhes pode consultar [7, 8].

Criptografia é a arte ou ciência de escrever mensagens em cifra ou em código, de modo que somente a pessoa autorizada possa decifrar e ler as mensagens.

A criptografia é tão antiga quanto a própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalhas. O mais interessante é que a tecnologia de criptografia não mudou muito até meados do século passado. Depois da Segunda Guerra Mundial, com a invenção do computador, a área realmente floresceu incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de mensagens. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

A mensagem a ser enviada é chamada de *texto-original* (plaintext) e a mensagem codificada é chamada de *texto-cifrado* (ciphertext). O texto-original e o texto-cifrado são

escritos em algum alfabeto $\mathbb{A}$ consistindo de um certo número n de símbolos; isto é,

$$\#(\mathbb{A}) = n.$$

O processo de converter um texto-original para um texto-cifrado é chamado de *codificação* ou *cifragem*, e o processo de reverter é chamado de *decodificação* ou *decifragem*.

O texto-original e texto-cifrado são divididos em mensagens unitárias. Uma mensagen unitária poder ser um bloco de k símbolos do alfabeto $\mathbb{A}$. O *processo de codificação* é uma função que associa cada mensagem unitária $\mathbf{u}$ do texto-original a uma mensagem unitária $\mathbf{c}$ do texto-cifrado. Mais precisamente, sejam $\mathcal{P}$ o conjunto de todas as possíveis mensagens unitárias $\mathbf{u}$ do texto-original e $\mathcal{C}$ o conjunto de todas as possíveis mensagens unitárias $\mathbf{c}$ do texto-cifrado. Então a correspondência biunívoca

$$f : \mathcal{P} \to \mathcal{C} \text{ tal que } f(\mathbf{u}) = \mathbf{c}$$

é o processo de codificação. A correspondência biunívoca

$$f^{-1} : \mathcal{C} \to \mathcal{P} \text{ tal que } f^{-1}(\mathbf{c}) = \mathbf{u}$$

é o processo de decodificação. Assim, temos o seguinte diagrama

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

Cripto-sistema

Um *Cripo-sistema* é qualquer bijeção de $\mathcal{P}$ sobre $\mathcal{C}$.

É útil substituir os símbolos de um alfabeto $\mathbb{A}$ por números inteiros $0, 1, 2, \ldots$, para tornar mais fácil a construção do cripto-sistema f. Uma correspondência natural entre o alfabeto

$$\mathbb{A} = \{A, B, C, \ldots, K, \ldots, X, Y, Z, \text{ espaço} = \sqcup\}$$

e o conjunto de números inteiros

$$\mathbb{Z}_{27} = \{0, 1, 2, \ldots, 10, \ldots, 23, 24, 25, 26\}$$

é dada pela tabela:

$$\begin{array}{cccccccccc} A & B & C & \cdots & K & \cdots & X & Y & Z & \sqcup \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & \cdots & 10 & \cdots & 23 & 24 & 25 & 26. \end{array} \tag{2.1}$$

Em geral, podemos rotular mensagens unitárias, com blocos de k símbolos, de um alfabeto $\mathbb{A}$ de n símbolos, por inteiros do conjunto

$$\mathbb{Z}_{n^k} = \{0, 1, \ldots, n^k - 1\}$$

do seguinte modo:

$$(x_{k-1}, \ldots, x_1, x_0) \in \mathbb{Z}_n^k \leftrightarrow x_{k-1}n^{k-1} + \cdots + x_1 n + x_0 n^0 \in \mathbb{Z}_{n^k},$$

onde cada x_i corresponde a um símbolo do alfabeto $\mathbb{A}$. Por exemplo, a mensagem unitária com bloco de quatro símbolos

$$\text{“}AQUI\text{”}$$

corresponde ao inteiro

$$0 \cdot 27^3 + 16 \cdot 27^2 + 20 \cdot 27 + 8 \cdot 27^0 = 12212 \in \mathbb{Z}_{27^4}.$$

Teorema 2.1 *Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}_n$ fixados. Se $\text{mdc}(a, n) = 1$, então a função*

$$f : \mathbb{Z}_n \to \mathbb{Z}_n \text{ dada por } f(x) = ax + b$$

é um cripto-sistema.

Prova. Como $\text{mdc}(a, n) = 1$ temos que existe $a' = a^{-1} \in \mathbb{Z}_n^*$ tal que $a \cdot a' = 1$. Assim,

$$f^{-1}(x) = a'x + b',$$

onde $b' = -a'b$, é tal que

$$f \circ f^{-1} = f^{-1} \circ f = I_{\mathbb{Z}_n};$$

isto é, f^{-1} é a função inversa de f. ■

Observação 2.1 *O cripto-sistema*

$$f(x) = ax + b$$

é chamado de transformação afim. *O par (a, b) é chamado de* chave de codificação *ou* chave secreta. *Quando $n = 27$, $a = 1$ e $b \in \mathbb{Z}_{27}$ o cripto-sistema*

$$f(x) = x + b$$

é chamado de Cifra de César, *pois Júlio César a utilizava para cifrar suas mensagens. Quando $b = 0$ o cripto-sistema*

$$f(x) = ax$$

é uma transformação linear.

Agora suponhamos que nossos textos - texto-original e texto-cifrado - são divididos em mensagens unitárias, com blocos de dois símbolos. Isto significa que o texto-original é dividido em segmentos de dois símbolos. Se o texto-original tem um número ímpar de símbolos, então para obter um número inteiro de blocos com dois símbolos adicionamos um símbolo extra no final; escolhemos um símbolo que não é provável para causar confusão, digamos espaço.

Exemplo 2.1 *Vamos primeiro estabelecer uma correspondência biunívoca entre o alfabeto* $\mathbb{A}$ *e números inteiros, pela tabela:*

$$\begin{array}{cccccccccc} A & B & C & \cdots & K & \cdots & X & Y & Z \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & \cdots & 10 & \cdots & 23 & 24 & 25. \end{array} \tag{2.2}$$

Seja o símbolo

$$x26 + y \in \mathbb{Z}_{676}$$

correspondendo uma mensagem unitária, com blocos de dois símbolos, do texto-original, onde $x \in \mathbb{Z}_{26}$ *corresponde ao primeiro símbolo da mensagem unitária e* $y \in \mathbb{Z}_{26}$ *corresponde ao segundo símbolo da mensagem unitária. Para* $a = 159$ *e* $b = 580$*, temos que a função*

$$f : \mathbb{Z}_{676} \to \mathbb{Z}_{676} \ \textit{dada por} \ f(z) = 159z + 580$$

é um cripo-sistema. Portanto, para codificar o texto-original

$$\text{“}AMOR\text{”},$$

primeiro dividimos o texto-original em blocos de dois símbolos e fazemos a correspondência numérica

$$\begin{array}{cc} AM & OR \\ \updownarrow & \updownarrow \\ 12 & 381. \end{array}$$

Agora, calculamos

$$f(12) = 460 = 17 \cdot 26 + 18 \ \ e \ \ f(381) = 319 = 12 \cdot 26 + 7,$$

logo a mensagem cifrada é

$$\text{“}RSMH\text{”}.$$

Um modo alternativo de transmitir mensagens unitárias, com blocos de dois símbolos, é fazer cada bloco de dois símbolos corresponder a um vetor

$$\mathbf{x} = \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{Z}_n^2.$$

Teorema 2.2 *Sejam* $n \in \mathbb{N}$,

$$A = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in M_2(\mathbb{Z}_n), B = \begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{Z}_n^2$$

e $D = \det(A)$. *Se* $\text{mdc}(n, D) = 1$, *então a função*

$$f : \mathbb{Z}_n^2 \to \mathbb{Z}_n^2 \text{ dada por } f(\mathbf{x}) = A\mathbf{x} + B,$$

é um cripto-sistema.

Prova. Temos, pelo Teorema 1.13, que a função

$$f : \mathbb{Z}_n^2 \to \mathbb{Z}_n^2 \text{ dada por } f(\mathbf{x}) = A\mathbf{x} + B,$$

é uma função invertível com inversa

$$f^{-1} : \mathbb{Z}_n^2 \to \mathbb{Z}_n^2 \text{ dada por } f^{-1}(\mathbf{x}) = A^{-1}\mathbf{x} - A^{-1}B.$$

■

Observação 2.2 *O Teorema acima pode ser generalizado para* $\mathbb{Z}_n^k$.

Exemplo 2.2 *A correspondência biunívoca entre o alfabeto* $\mathbb{A}$ *e números inteiros é dada pela tabela* 2.2. *Seja o vetor*

$$\mathbf{x} = \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{Z}_{26}^2$$

correspondendo uma mensagem unitária, com blocos de dois símbolos, do texto-original, onde $x \in \mathbb{Z}_{26}$ *corresponde ao primeiro símbolo da mensagem unitária e* $y \in \mathbb{Z}_{26}$ *corresponde ao segundo símbolo da mensagem unitária. Assim, com*

$$A = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \in M_2(\mathbb{Z}_{26}) \text{ e } B = \begin{bmatrix} 7 \\ 11 \end{bmatrix} \in \mathbb{Z}_n^2$$

temos que a função

$$f : \mathbb{Z}_{26}^2 \to \mathbb{Z}_{26}^2 \text{ dada por } f(\mathbf{x}) = A\mathbf{x} + B$$

é um cripto-sistema. Portanto, para codificar o texto-original

$$\text{“}JA\text{”},$$

primeiro fazemos a correspondência do texto-original com o vetor

$$\mathbf{x} = \begin{bmatrix} 9 \\ 0 \end{bmatrix} \in \mathbb{Z}_{26}^2$$

e depois calculamos

$$f(\mathbf{x}) = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 9 \\ 0 \end{bmatrix} + \begin{bmatrix} 7 \\ 11 \end{bmatrix} = \begin{bmatrix} 25 \\ 22 \end{bmatrix},$$

logo a mensagem cifrada é

$$\text{“}ZW\text{”}.$$

Observação 2.3 *Para codificar um texto-original, com m blocos de dois símbolos, podemos escrevê-lo como uma matriz $2 \times m$, onde cada coluna corresponde a um vetor de $\mathbb{Z}_n^2$, e usar o seguinte cripto-sistema*

$$f : M_{2\times m}(\mathbb{Z}_n) \to M_{2\times m}(\mathbb{Z}_n)$$

dado por

$$f([\ \mathbf{x}_1 \ \cdots \ \mathbf{x}_m\ ]) = [\ A\mathbf{x}_1 + B \ \cdots \ A\mathbf{x}_m + B\ ].$$

Exemplo 2.3 *Vamos continuar o exemplo acima. Assim, para codificar o texto-original*

$$\text{“}RONDONOPOLIS\text{”},$$

primeiro fazemos a correspondência do texto-original com a matriz 2×6

$$\begin{bmatrix} 17 & 13 & 14 & 14 & 14 & 8 \\ 14 & 3 & 13 & 15 & 11 & 18 \end{bmatrix}$$

e depois calculamos

$$f(\begin{bmatrix} 17 & 13 & 14 & 14 & 14 & 8 \\ 14 & 3 & 13 & 15 & 11 & 18 \end{bmatrix}) = \begin{bmatrix} 5 & 16 & 22 & 2 & 16 & 25 \\ 8 & 22 & 5 & 21 & 15 & 3 \end{bmatrix},$$

logo a mensagem cifrada é

$$\text{“}FIQWWFCVQPZD\text{”}.$$

Um *codificador por substituição* com período p consiste de p cripo-sistemas $f_i : \mathcal{P} \to \mathcal{C}_i$, $i = 1, \ldots, p$. Uma mensagem

$$\mathbf{u} = (u_1, \ldots, u_p, u_{p+1}, \ldots, u_{2p}, \ldots)$$

é codificada como

$$\mathbf{c} = (f_1(u_1), \ldots, f_p(u_p), f_1(u_{p+1}), \ldots, f_p(u_{2p}), \ldots).$$

Por vários séculos um dos métodos mais populares de codificação por substituição foi a *Cifra de Vigenère*. Neste sistema de codificação, primeiro escolhemos um vetor

$$\mathbf{b} \in \mathbb{Z}_n^p,$$

onde $\mathbf{b}$ corresponde a uma palavra de fácil memorização, chamada de *palavra-chave* e depois usamos o cripto-sistema

$$f : \mathbb{Z}_n^p \to \mathbb{Z}_n^p \text{ dado por } f(\mathbf{x}) = \mathbf{x} + \mathbf{b}.$$

Um modo prático para obter a Cifra de Vigenère é através do Arranjo Circulante dado na Tabela 2.3.

$$\begin{array}{ccccc} A & B & \cdots & Y & Z \\ B & C & \cdots & Z & A \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ Y & Z & \cdots & W & X \\ Z & A & \cdots & X & Y \end{array} \tag{2.3}$$

Exemplo 2.4 *A correspondência biunívoca entre o alfabeto* $\mathbb{A}$ *e números inteiros é dada pela tabela* 2.1*. Agora escolhemos uma palavra-chave, digamos*

$$\text{“}AMO\text{”},$$

a qual corresponde ao vetor

$$\mathbf{b} = (0, 12, 14) \in \mathbb{Z}_{27}^3.$$

Assim, usando o Arranjo Circulante dado na Tabela 2.4 *para cifrar o texto-original*

$$\text{“}JOAO\ PESSOA\ CIDADE\ VERDE\text{”}$$

obtemos a mensagem cifrada

$$\text{“}J \sqcup OOLCETFOMNCURAPS \sqcup GSRPS\text{”},$$

a qual corresponde a

$$\text{“}f_1(J)f_2(O)f_3(A)f_1(O)f_2(\sqcup)f_3(P)\cdots f_1(\sqcup)f_2(V)f_3(E)f_1(R)f_2(D)f_3(E)\text{”}.$$

Neste caso, os cripo-sistemas $f_i : \mathbb{Z}_{27} \to \mathbb{Z}_{27}$, $i = 1, 2, 3$, *são dados por* $f_1(x) = x$, $f_2(x) = x + 12$ *e* $f_3(x) = x + 14$, *isto é, os* f_i *são Cifras de César.*

$$\begin{array}{cccccl} A & B & C & \cdots & \sqcup & \\ A & B & C & \cdots & \sqcup & = f_1(A)f_1(B)f_1(C)\cdots f_1(\sqcup) \\ M & N & O & \cdots & L & = f_2(A)f_2(B)f_2(C)\cdots f_2(\sqcup) \\ O & P & Q & \cdots & N & = f_3(A)f_3(B)f_3(C)\cdots f_3(\sqcup) \end{array} \tag{2.4}$$

Os sistemas clássicos de Criptografia, como a Cifra de César e de Vigenère, são todos simétricos; isto é, a chave usada para a codificação é igual à chave usada para a decodificação ou, equivalentemente, a partir de uma delas a outra é obtida facilmente. Nestes sistemas, conhecendo a chave de codificação

$$(a, b)$$

podemos calcular a chave de decodificação

$$(a^{-1} \bmod n^k, -a^{-1}b \bmod n^k)$$

pelo Algoritmo Euclidiano. Note que, estes sistemas são difíceis de serem “quebrados”, pois a chave é usada apenas uma vez para cada texto-original. Portanto, os sistemas simétricos são interessantes quando um transmissor conversa apenas com o mesmo receptor. Caso um transmissor converse com vários receptores e a chave de codificação seja mantida constante, então todos os receptores estarão aptos para decodificar o texto-cifrado. Caso a chave de codificação não seja mantida constante, então o sistema torna-se inviável.

2.2 Sistema DH

Sistemas criptográficos com chaves públicas foram proposto por Diffie e Hellman (DH) em 1976. Os sistemas criptográficos com chaves públicas DH se caracterizam por duas chaves diferentes: a chave (chave de codificação) da transmissora é pública e a chave (chave de decodificação) da receptora é secreta. Portanto, os sistemas criptográficos com

chaves públicas possuem uma estrutura assimétrica, isto é, a obtenção de uma chave a partir da outra, se constitui em um problema não realizável.

Os sistemas criptográficos com chaves públicas opera do seguinte modo: um usuário u_i desejando se comunicar com um usuário u_j de maneira secreta, envia uma solicitação para início de comunicação. O usuário u_j determina um par de chaves $k_{c,j}$ e $k_{d,j}$ tais que

$$k_{d,j} \circ k_{c,j}(\mathbf{u}) = \mathbf{u} \text{ e } k_{c,j} \circ k_{d,j}(\mathbf{u}) = \mathbf{u}$$

onde a chave $k_{d,j}$ é mantida secreta e usada para a decodificação, enquanto a chave $k_{c,j}$ é tornada pública e usada para a codificação. O usuário u_j obtém a chave pública $k_{c,j}$ e, assim, passa a codificar mensagens unitárias para o usuário u_j, pois só este conhece a chave secreta $k_{d,j}$. Estes processos de codificação e decodificação deverão satisfazer as seguintes condições:

1. O cálculo do par de chaves $k_{c,j}$ e $k_{d,j}$ deve ser simples;

2. O usuário (transmissor) u_i deve realizar a operação de codificação facilmente; isto é,

$$\mathbf{c} = k_{c,j}(\mathbf{u});$$

3. O usuário (receptor) u_j deve realizar a operação de decodificação facilmente; isto é,

$$\mathbf{u} = k_{d,j}(\mathbf{c});$$

4. É praticamente impossível descobrir $k_{d,j}$ a partir de $k_{c,j}$. É claro que dada $k_{c,j}$ temos uma maneira de descobrir $k_{d,j}(\mathbf{c})$, basta codificar toda mensagem unitária $\mathbf{u}$ e quando $\mathbf{c} = k_{c,j}(\mathbf{u})$, teremos que $\mathbf{u} = k_{d,j}(\mathbf{c})$ mas isto torna-se inviável.

Em um sistema de criptografia com chave pública DH, dois usuários u_i e u_j desejam formar uma chave secreta k_{ij}, onde u_i tem uma chave secreta $k_{d,i}$ e u_j tem uma chave secreta $k_{d,j}$. Primeiro eles escolhem um sistema de parâmetros público: um número primo p extremamente grande (com aproximadamente 100 dígitos) e t um elemento primitivo módulo p, isto é,

$$\text{mdc}(t, p) = 1.$$

A seguir o usuário u_i calcula

$$k_{c,i} \equiv t^{k_{d,i}} \pmod{p},$$

e envia $k_{c,i}$. Similarmente, o usuário u_j calcula

$$k_{c,j} \equiv t^{k_{d,j}} \pmod{p},$$

e envia $k_{c,j}$. Finalmente, calculam

$$\begin{aligned} k_{ij} &\equiv t^{k_{d,i}k_{d,j}} \pmod{p} \\ &\equiv k_{c,i}^{k_{d,j}} \pmod{p} \\ &\equiv k_{c,j}^{k_{d,i}} \pmod{p}. \end{aligned}$$

Portanto, ambos u_i e u_j são capazes de calcular k_{ij}.

Exemplo 2.5 *Sejam* $t = 6$ *um elemento primitivo* $(\mathrm{mod}\, 733)$, $k_{d,i} = 29$ *e* $k_{d,j} = 19$ *as chaves de decodificação dos usuários* u_i *e* u_j, *respectivamente. Então o usuário* u_i *calcula a chave de codificação*

$$\begin{aligned} k_{c,i} &\equiv t^{k_{d,i}} \pmod{733} \\ k_{c,i} &\equiv 6^{29} \pmod{733} \\ k_{c,i} &\equiv 578 \pmod{733} \end{aligned}$$

e envia $k_{c,i} = 578$. *Do mesmo modo, o usuário* u_j *calcula*

$$\begin{aligned} k_{c,j} &\equiv t^{k_{d,j}} \pmod{733} \\ k_{c,j} &\equiv 6^{19} \pmod{733} \\ k_{c,j} &\equiv 327 \pmod{733} \end{aligned}$$

e envia $k_{c,j} = 327$. *Finalmente calculam*

$$\begin{aligned} k_{ij} &\equiv t^{k_{d,i}k_{d,j}} \pmod{733} \\ k_{ij} &\equiv 6^{19.29} \pmod{733} \\ k_{ij} &\equiv 247 \pmod{733}. \end{aligned}$$

Agora, suponhamos que u_i deseje enviar a u_j uma mensagem $\mathbf{u}$, onde $1 \leq \mathbf{u} \leq p-1$. Primeiro, u_i escolhe uma chave secreta $k_{d,i}$, isto é, um número aleatório $k_{d,i}$ tal que

$$1 \leq k_{d,i} \leq p-1.$$

A seguir u_i calcula

$$k_{ij} \equiv k_{c,j}^{k_{d,i}} \pmod{p},$$

onde $k_{c,j} \equiv t^{k_{d,j}} \pmod{p}$ está em um arquivo público ou é enviada por u_j. O texto-cifrado é o par

$$\mathbf{c} = (c_1, c_2),$$

onde

$$c_1 \equiv t^{k_{d,i}} \pmod{p} \text{ e } c_2 \equiv k_{ij}\mathbf{u} \pmod{p}. \tag{2.5}$$

É aconselhável utilizar chaves de decodificacão $k_{d.i}$ diferentes, para cada mensagem $\mathbf{u}$ do texto-original.

O processo de decodificação é composto de duas etapas. Primeira etapa: recuperar k_{ij}, isto é, calcular

$$\begin{aligned} k_{ij} &\equiv t^{k_{d,i}k_{d,j}} \pmod{p} \\ &\equiv c_1^{k_{d,j}} \pmod{p}. \end{aligned}$$

Mas isto é fácil, pois $k_{d,j}$ é conhecida somente por u_j. Segunda etapa: divide c_2 por k_{ij} para recuperar $\mathbf{u}$.

Exemplo 2.6 *A correspondência entre o alfabeto $\mathbb{A}$ e números inteiros é dada pela tabela 2.1. Sejam $t = 6$ um elemento primitivo $\pmod{733}$, $k_{d,i_1} = 29$, $k_{d,i_2} = 8$ e $k_{d,j} = 19$ as chaves de decodificação, $k_{c,i} = 578$ e $k_{c,j} = 327$ as chaves de codificação dos usuários u_i e u_j, respectivamente. Assim, para codificar o texto-original*

$$\text{“}AMOR\text{”}$$

dividido em blocos de dois símbolos, com correspondência numérica

$$\begin{array}{cc} AM & OR \\ \updownarrow & \updownarrow \\ 12 & 395 \end{array}$$

o usuário u_i calcula

$$k_{(ij)_1} \equiv 247 \pmod{733}$$

e

$$k_{(ij)_2} \equiv 373 \pmod{733}.$$

A seguir calcula

$$\begin{aligned} c_{11} &\equiv t^{k_{d,i_1}} \equiv 6^{29} \equiv 578 \,(\mathrm{mod}\, 733) \\ c_{12} &\equiv k_{(ij)_1} \cdot \mathbf{u}_1 \equiv 247 \cdot 12 \equiv 32 \,(\mathrm{mod}\, 733) \\ c_{21} &\equiv t^{k_{d,i_2}} \equiv 6^{8} \equiv 313 \,(\mathrm{mod}\, 733) \\ c_{22} &\equiv k_{(ij)_2} \cdot \mathbf{u}_2 \equiv 313 \cdot 395 \equiv 2 \,(\mathrm{mod}\, 733). \end{aligned}$$

Logo, o texto-cifrado são os pares

$$c_1 = (c_{11}, c_{12}) \;\; e \;\; c_2 = (c_{21}, c_{22})$$

onde

$$\begin{aligned} c_{11} &\equiv 578 \equiv 21 \cdot 27 + 11 \,(\mathrm{mod}\, 733) \\ c_{12} &\equiv 32 \equiv 1 \cdot 27 + 5 \,(\mathrm{mod}\, 733) \\ c_{21} &\equiv 313 \equiv 11 \cdot 27 + 16 \,(\mathrm{mod}\, 733) \\ c_{22} &\equiv 2 \equiv 0 \cdot 27 + 2 \,(\mathrm{mod}\, 733). \end{aligned}$$

Portanto, o usuário u_i envia para o usuário u_j, o texto-cifrado

$$\text{“}VLBFLQAC\text{”}.$$

Para decodificar o texto-cifrado com correspondência numérica

$$\begin{array}{cccccccc} V & L & B & F & L & Q & A & C \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 21 & 11 & 1 & 5 & 11 & 16 & 0 & 2 \end{array},$$

o usuário u_j recupera

$$c_{11} = 578, c_{12} = 32, c_{21} = 313 \;\; e \;\; c_{22} = 2.$$

A seguir calcula

$$(c_{11})^{k_{d,j}} \equiv 578^{19} \equiv 247 \equiv k_{(ij)_1} \,(\mathrm{mod}\, 733)$$

e

$$\mathbf{u}_1 \equiv \frac{c_{12}}{k_{(ij)_1}} \equiv 32 \cdot 92 \equiv 12 \,(\mathrm{mod}\, 733).$$

Do mesmo modo calcula

$$(c_{21})^{k_{d,j}} \equiv 313^{19} \equiv 373 \equiv k_{(ij)_2} \,(\mathrm{mod}\, 733)$$

e

$$\mathbf{u}_2 \equiv \frac{c_{22}}{k_{(ij)_2}} \equiv 2 \cdot 564 \equiv 395 \pmod{733}.$$

Como

$$\mathbf{u}_1 \equiv 12 \equiv 0 \cdot 27 + 12 \pmod{733}$$

e

$$\mathbf{u}_2 \equiv 395 \equiv 14 \cdot 27 + 17 \pmod{733},$$

o texto-original é

$$\begin{array}{cccc} A & M & O & R \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 12 & 14 & 17 \end{array}.$$

Note que, o tamanho do texto-cifrado é o dobro do tamanho do texto-original. Também note que, a operação de multiplicação em 2.5, pode ser substituída por qualquer outra operação invertível tal como adição módulo p.

O arquivo público consiste de uma entrada para cada usuário u_i, a saber $k_{c,i}$, pois t e p são conhecidos por todos os usuários.

2.3 Sistema de Distribuição GH-PKD

Nesta seção apresentaremos um sistema de distribuição com chave pública (GH-PKD) proposto por Gong e Harn em [6], que é construido por um par de seqüências características de ordem 3.

O sistema de distribuição GH-PKD é um sistema de criptografia com chave pública, que tem como parâmetros público um número primo p e um polinômio

$$f = x^3 - ax^2 + bx - 1$$

irredutível sobre $\mathbb{F}_p$, com período

$$Q = p^2 + p + 1.$$

Neste sistema, um usuário u_i escolhe aleatoriamente $r_i \in \mathbb{Z}$ tal que

$$0 < r_i < Q \text{ e } \operatorname{mdc}(r_i, Q) = 1.$$

A seguir u_i calcula (s_{r_i}, s_{-r_i}) do sistema com chave pública e parâmetros

$$p \text{ e } f = x^3 - ax^2 + bx - 1.$$

Agora, o usuário u_i torna público a chave de codificação

$$k_{c,i} = (s_{r_i}, s_{-r_i})$$

e mantém secreta a chave de decodificação $k_{d,i} = r_i$. Da mesma forma, um usuário u_j escolhe aleatoriamente $r_j \in \mathbb{Z}$ tal que

$$0 < r_j < Q \text{ e } \operatorname{mdc}(r_j, Q) = 1.$$

A seguir u_j calcula $\left(s_{r_j}, s_{-r_j}\right)$ do sistema com chave pública

$$p \text{ e } f(x) = x^3 - ax^2 + bx - 1.$$

Agora, o usuário u_j torna público a chave de codificação

$$k_{c,j} = (s_{r_j}, s_{-r_j})$$

e mantém secreta a chave de decodificação $k_{d,j} = r_j$. Assim, pelo Lema 1.10, ambos u_i e u_j são capazes de calcular

$$s_{r_i}\left(s_{r_j}, s_{-r_j}\right) = s_{r_i r_j} = s_{r_j}\left(s_{r_i}, s_{-r_i}\right),$$

e

$$s_{-r_i}\left(s_{r_j}, s_{-r_j}\right) = s_{-r_i r_j} = s_{-r_j}\left(s_{r_i}, s_{-r_i}\right).$$

Portanto, a chave comum dos usuários u_i e u_j é

$$k_{ij} = \left(s_{r_i r_j}, s_{-r_i r_j}\right).$$

Exemplo 2.7 *Sejam* $p = 11$, $f = x^3 + 4x - 1$ *um polinômio irredutível sobre* $\mathbb{F}_{11}$ *de período* $133 = 7 \times 19$, $r_i = 9$ *e* $r_j = 13$ *as chaves de decodificação dos usuários* u_i *e* u_j, *respectivamente. Então o usuário* u_i *calcula*

$$\begin{aligned} k_{c,i} &= (s_{r_i}, s_{-r_i}) \\ &= (s_9, s_{-9}) \\ &= (10, 6) \end{aligned}$$

e torna público sua chave de codificação $k_{c,i}$. Do mesmo modo, o usuário u_j calcula

$$\begin{aligned} k_{c,j} &= \left(s_{r_j}, s_{-r_j}\right) \\ &= (s_{13}, s_{-13}) \\ &= (7,1) \end{aligned}$$

e torna público sua chave de codificação $k_{c,j}$. A seguir, o usuário u_i calcula

$$s_{r_i}\left(s_{r_j}, s_{-r_j}\right) = s_9\,(7,1) = 8$$

e

$$\begin{aligned} s_{-r_i}\left(s_{r_j}, s_{-r_j}\right) &= s_{-9}\,(7,1) \\ &= s_{124}\,(7,1) \\ &= 5. \end{aligned}$$

Assim, ele obtém a chave comum

$$k_{ij} = (8,5)\,.$$

Do mesmo modo, o usuário u_j calcula

$$s_{r_j}\left(s_{r_i}, s_{-r_i}\right) = s_{13}\,(10,6) = 8$$

e

$$\begin{aligned} s_{-r_j}\left(s_{r_i}, s_{-r_i}\right) &= s_{-13}\,(10,6) \\ &= s_{120}\,(10,6) \\ &= 5. \end{aligned}$$

Portanto, ele obtém a mesma chave comum

$$k_{ij} = (8,5)$$

do usuário u_i.

Observação 2.4 *1. Na fase de distribuição de chave*

$$\left[\begin{array}{ccc} u_i \ \textit{calcula} & \overset{(s_{r_i}, s_{-r_i})}{\longrightarrow} & u_j \ \textit{calcula} \\ \\ s_{r_i}\left(s_{r_j}, s_{-r_j}\right) \ \textit{e} \ s_{-r_i}\left(s_{r_j}, s_{-r_j}\right) & \overset{(s_{r_j}, s_{-r_j})}{\longleftarrow} & s_{r_j}\left(s_{r_i}, s_{-r_i}\right) \ \textit{e} \ s_{-r_j}\left(s_{r_i}, s_{-r_i}\right) \end{array}\right]$$

o sistema de distribuição com chave pública (GH-PKD) não envolve

$$f(x) = x^3 - ax^2 + bx - 1$$

do sistema de parâmetros público.

2. *Os espaços das chaves secretas e chaves públicas são os conjuntos*

$$\{lp^i \pmod{Q} : i = 0, 1, 2 \ \ e \ \ l \in \mathbb{Z}_+\}.$$

consistindo de todos os líderes de classe módulo $Q = p^2 + p + 1$ *relativamente primo com* Q *e todos os polinômios irredutíveis sobre* $\mathbb{F}_p$ *de grau* 3 *com período* Q*, respectivamente. Pelo Teorema* 1.26*, a aplicação*

$$k \leftrightarrow (s_k, s_{-k})$$

do espaço das chaves privadas para o espaço das chaves pública é bijetora. Assim haverá diferentes chaves públicas correspondendo a diferentes chaves secretas em GH-PKD.

3. *O tamanho do espaço das chaves secretas (ou públicas) é*

$$\frac{\varphi(p^2 + p + 1)}{3}.$$

Exemplo 2.8 *Vamos continuar o Exemplo* 2.7*. A correspondência entre o alfabeto* $\mathbb{A}$ *e números inteiros é dada pela tabela* 2.1*. Assim, para codificar o texto-original*

$$\text{“}JA\text{”},$$

com correspondência numérica

$$\begin{array}{cc} J & A \\ \updownarrow & \updownarrow \\ 9 & 0 \end{array}$$

o usuário $\mathbf{u}_i$ *calcula*

$$k_{ij} = (8, 5).$$

A seguir calcula

$$\begin{aligned} c_1 &= (s_{r_i}, s_{-r_i}) = (s_9, s_{-9}) = (10, 6) \\ c_2 &= k_{ij} + u = (8, 5) + (9, 0) = (17, 5). \end{aligned}$$

Logo, o texto-cifrado é o par

$$\mathbf{c} = (c_1, c_2)\,.$$

Portanto, o usuário $\mathbf{u}_i$ *envia para o usuário* $\mathbf{u}_j$*, o texto-cifrado*

$$\text{“}KGRF\text{”}.$$

Para decodificar o texto-cifrado com correspondência numérica

$$\begin{array}{cccc} K & G & R & F \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 10 & 6 & 17 & 5 \end{array},$$

o usuário $\mathbf{u}_j$ *recupera*

$$c_1 = (10, 6) \;\; e \;\; c_2 = (17, 5).$$

A seguir calcula

$$s_{13}(10, 6) = 8 \;\; e \;\; s_{-13}(10, 6) = 5$$

para obter chave comum

$$k_{ij} = (8, 5)$$

e calcula

$$\mathbf{u} = c_2 - k_{ij} = (17, 5) - (8, 5) = (9, 0)\,.$$

Portanto, o texto-original é

$$\begin{array}{cc} J & A \\ \updownarrow & \updownarrow \\ 9 & 0 \end{array}.$$

Capítulo 3

Sistema de Codificação do Tipo RSA

Nesta capítulo iremos propor um cripto-sistema com chave pública do tipo RSA, usando um par de seqüências característica sobre $\mathbb{Z}_n$.

3.1 Sistema RSA

Nesta seção apresentaremos um sistema de criptografia com chave pública proposto por Rivest, Shamir e Adleman (RSA) em [11]. O leitor interessado em mais detalhes pode consultar [7, 8].

Em um sistema de criptografia com chave pública RSA, cada usuário u_i escolhe dois números primos distintos extremamente grandes p_i e q_i (com aproximadamente 100 dígitos cada) e aleatoriamente um número t_i tal que

$$\text{mdc}(t_i, (p_i - 1)(q_i - 1)) = 1.$$

A seguir u_i calcula

$$n_i = p_i q_i \text{ e } \varphi(n_i) = \varphi(p_i)\varphi(q_i) = n_i + 1 - (p_i + q_i),$$

e também

$$r_i \equiv t_i^{-1} \pmod{\varphi(n_i)}.$$

Agora, o usuário u_i torna público a chave de codificação

$$k_{c,i} = (n_i, t_i)$$

e mantém secreta a chave de decodificação

$$k_{d,i} = (n_i, r_i).$$

O processo de codificação é dado pela função

$$f : \mathbb{Z}_{n_i} \to \mathbb{Z}_{n_i},\ f(x) = x^{t_i}$$

e, pelo Corolário 1.2, o processo de decodificação é dado pela função

$$f^{-1} : \mathbb{Z}_{n_i} \to \mathbb{Z}_{n_i},\ \ f(x) = x^{r_i}.$$

Seja $\mathbb{A}$ um alfabeto com n símbolos. Na prática queremos trabalhar com $\mathcal{P} \neq \mathcal{C}$. Assim, vamos dividir nosso texto-original em mensagens unitárias com blocos de k símbolos, os quais são vistos como um inteiro

$$x = x_{k-1}n^{k-1} + \cdots + x_1 n + x_0 n^0 \in \mathbb{Z}_{n^k}, x_r \in \{0, 1, \ldots, n-1\},$$

e cada um destes blocos será codificado em um só bloco com l símbolos, onde $k < l$. Para fazer isto cada usuário u_i escolhe dois números primos distintos p_i e q_i de modo que $n_i = p_i q_i$ satisfaça

$$n^k < n_i < n^l.$$

Então qualquer mensagem unitária $\mathbf{u}$ do texto-original isto é, um inteiro menor do que n^k, corresponde a um elemento de $\mathbb{Z}_{n_i}$ e, como $n_i < n^l$, a imagem $f(\mathbf{u}) \in \mathbb{Z}_{n_i}$ pode ser escrita de modo único como um bloco de l símbolos. Note que nem todos os blocos de l símbolos são usados, mas apenas aqueles correspondendo aos inteiros menores do que n^k para cada usuário u_i.

Exemplo 3.1 *A correspondência biunívoca entre o alfabeto $\mathbb{A}$ e números inteiros é dada pela Tabela 2.2 e escolhemos $k = 3$ e $l = 4$. Para enviar o texto-original*

$$\text{“}AMO\text{”}$$

para um usuário u_j com chave de codificação

$$k_{c,j} = (46927, 39423),$$

primeiro determinamos a equivalência numérica

$$AMO$$
$$\updownarrow$$
$$326$$

e então calculamos

$$326^{39423} \pmod{46927} = 41309.$$

Como

$$41309 = 2 \cdot 26^3 + 9 \cdot 26^2 + 2 \cdot 26 + 21$$

temos que o texto-cifrado é

$$\text{“}CJCV\text{”}.$$

O receptor u_j conhece a chave de decodificação

$$k_{d,j} = (46927, 26767)$$

e assim calcula

$$41309^{26767} \pmod{46927} = 326.$$

Como

$$326 = 0 \cdot 26^2 + 12 \cdot 26 + 14$$

temos que o texto-original é

$$\text{“}AMO\text{”}.$$

Como o usuário u_i gerou suas chaves? Primeiro ele multiplicou os números primos $p_i = 281$ e $q_i = 167$ para obter n_i; então escolheu t_i aleatoriamente tal que

$$\text{mdc}(t_i, p_i - 1) = \text{mdc}(t_i, q_i - 1) = 1.$$

Finalmente determinou

$$r_i \equiv t_i^{-1} \pmod{(p_i - 1)(q_i - 1)}.$$

Note que os números p_i, q_i e r_i permanecem secretos.

Notamos que uma desvantagem dos sistemas de criptografia com chave pública é que são bem mais lentos do que os sistemas de criptografia clássicos, pois eles usam potências ao invés de somas. Em compensação, por isso mesmo, são mais seguros. Note, também, que um modo de calcular a chave secreta (n, r) a partir da chave pública (n, t) é fatorar n em fatores primos e depois recupera r tal que

$$rt \equiv 1 \pmod{\varphi(n)}.$$

O ponto importante neste procedimento é que não se conhece um algoritmo rápido para determinar a decomposição de n.

3.2 Sistema de Codificação do Tipo RSA

Nesta seção apresentaremos um cripto-sistema com chave pública do tipo RSA, usando um par de seqüências recursivas lineares homogêneas de ordem 3 sobre $\mathbb{Z}_n$, proposto por Gong e Harn em [6].

Seja

$$s_k = as_{k-1} - bs_{k-2} + s_{k-3}, \forall k = 3, 4, \ldots$$

uma seqüência recursiva linear homogênea de ordem 3 sobre $\mathbb{F}_p$ com polinômio característico

$$f = x^3 - ax^2 + bx - 1.$$

Então o período $\mathrm{per}\,(\mathbf{s})$ da seqüência $\mathbf{s}$ satisfaz um dos seguintes casos:

1º **Caso** f é redutível sobre $\mathbb{F}_p$ se, e somente se,

$$\mathrm{per}\,(\mathbf{s}) \mid p - 1.$$

2º **Caso** $f = (x - \alpha)\, f_1$, onde f_1 é irredutível sobre $\mathbb{F}_p$ e $\alpha \in \mathbb{F}_p$ se, e somente se,

$$\mathrm{per}\,(\mathbf{s}) \mid p^2 - 1 \text{ e } \mathrm{per}\,(\mathbf{s}) \nmid p - 1.$$

3º **Caso** f é irredutível sobre $\mathbb{F}_p$ se, e somente se,

$$\mathrm{per}\,(\mathbf{s}) \mid p^2 + p + 1.$$

De acordo com o método para resolver equações cúbicas sobre $\mathbb{F}_p$ (cf. [**?**]), substituindo

$$x = y + 3^{-1}a$$

em

$$f = x^3 - ax^2 + bx - 1,$$

obtemos que

$$f = g(y) = y^3 + C(a, b)y + D(a, b) \tag{3.1}$$

onde

$$C\,(a, b) = 3^{-1}a^2 + b \text{ e } D(a, b) = -2 \cdot 3^{-1}a^3 + 3^{-1}ab - 1.$$

O discriminante da cúbica 3.1 é definido por

$$\Delta(a,b) = -4C^3(a,b) - 27D^2(a,b).$$

Seja $m \in \{p,q\}$. Então,

$$\gamma(a,b) = \left(\frac{-27D(a,b) + \sqrt{-27\Delta(a,b)}}{-27D(a,b) - \sqrt{-27\Delta(a,b)}}\right)^{2N},$$

onde

$$N \in \left\{\frac{(m-1)}{6}, \frac{(m+1)}{6}\right\}$$

Como todos os cálculos são realizados em $\mathbb{Z}_n$, onde $n = pq$, vamos definir a função lógica

$$\Gamma(j,m), j \in \{1,2,3\} \text{ e } m \in \{p,q\}.$$

(i) $\Gamma(1,m)$ é verdade se, e somente se,

$$\Delta(c_1,c_2) \equiv 0 \pmod{m}$$

ou

$$\Delta(c_1,c_2) \not\equiv 0 \pmod{m}, \left(\frac{\Delta(c_1,c_2)}{m}\right) = 1 \text{ e } \gamma(c_1,c_2) \equiv 1 \pmod{m}$$

se, e somente se, 1º **Caso**.

(ii) $\Gamma(2,m)$ é verdade se, e somente se,

$$\Delta(c_1,c_2) \not\equiv 0 \pmod{m} \text{ e } \left(\frac{\Delta(c_1,c_2)}{m}\right) = -1$$

se, e somente se, 2º **Caso**.

(iii) $\Gamma(3,m)$ é verdade se, e somente se,

$$\Delta(c_1,c_2) \not\equiv 0 \pmod{m}, \left(\frac{\Delta(c_1,c_2)}{m}\right) = 1 \text{ e } \gamma(c_1,c_2) \not\equiv 1 \pmod{m}$$

se, e somente se, 3º **Caso**.

Vamos denotar os períodos de cada caso por

$$R_{1,m} = m-1,\ R_{2,m} = m^2-1 \text{ e } R_{3,m} = m^2+m+1.$$

Neste sistema de criptografia com chave pública do tipo RSA, cada usuário u_i escolhe dois números primos distintos extremamente grandes p_i e q_i (com aproximadamente 100 dígitos cada) e aleatoriamente um número t_i tal que

$$\text{mdc}(t_i, p_i^l - 1) = \text{mdc}(t_i, q_i^l - 1) = 1, l = 2,3.$$

Agora, o usuário u_i torna público a chave de codificação

$$k_{c,i} = (n_i, t_i)$$

e mantém secreta a chave de decodificação

$$k_{d,i} = (n_i, d_r).$$

O processo de codificação é dado por

$$c_1 = s_{t_i}(u_1, u_2) \text{ e } c_2 = s_{-t_i}(u_1, u_2).$$

Logo, o texto cifrado é o par

$$\mathbf{c} = (c_1, c_2).$$

Observação 3.1 *De acordo com o Fato* 1.1 *e o Teorema* 1.11*, a correspondência*

$$(u_1, u_2) \leftrightarrow (c_1, c_2)$$

entre o texto-original o texto-cifrado é biunívoca.

O processo de decodificação é composto de algumas etapas. Primeiro u_i calcula

$$D(c_1, c_2) = -2 \cdot 3^{-3} c_1^3 + 3^{-1} c_1 c_2 - 1$$

e

$$\Delta(c_1, c_2) = 4C^3(c_1, c_2) - 27D^2(c_1, c_2)$$

onde

$$C(c_1, c_2) = 3^{-1} c_1^3 + c_2.$$

A seguir calcula

$$\gamma(c_1, c_2) = \left(\frac{-27D(c_1, c_2) + \sqrt{-27\Delta(c_1, c_2)}}{-27D(c_1, c_2) - \sqrt{-27\Delta(c_1, c_2)}} \right)^{2N}$$

onde $N \in \left\{ \frac{(m-1)}{6}, \frac{(m+1)}{6} \right\}$ e $m \in \{p, q\}$. Assim, u_i escolhe a chave de decodificação apropriada

$$k_{d,i} = (n_i, d_r)$$

na Tabela 3.1 e calcula

$$u_1 = s_{d_r}(c_1, c_2) \text{ e } u_2 = s_{-d_r}(c_1, c_2).$$

Condição	Multiplicador do Período	Chave de Decodificação
$\Gamma(1,p) \wedge \Gamma(1,q)$	$\delta_1 = R_{1,p} \cdot R_{1,q}$	$d_1 t \equiv 1 \pmod{\delta_1}$
$\Gamma(1,p) \wedge \Gamma(2,q)$	$\delta_2 = R_{1,p} \cdot R_{2,q}$	$d_2 t \equiv 1 \pmod{\delta_2}$
$\Gamma(1,p) \wedge \Gamma(3,q)$	$\delta_3 = R_{1,p} \cdot R_{3,q}$	$d_3 t \equiv 1 \pmod{\delta_3}$
$\Gamma(2,p) \wedge \Gamma(1,q)$	$\delta_4 = R_{2,p} \cdot R_{1,q}$	$d_4 t \equiv 1 \pmod{\delta_4}$
$\Gamma(2,p) \wedge \Gamma(2,q)$	$\delta_5 = R_{2,p} \cdot R_{2,q}$	$d_5 t \equiv 1 \pmod{\delta_5}$
$\Gamma(2,p) \wedge \Gamma(3,q)$	$\delta_6 = R_{2,p} \cdot R_{3,q}$	$d_6 t \equiv 1 \pmod{\delta_6}$
$\Gamma(3,p) \wedge \Gamma(1,q)$	$\delta_7 = R_{3,p} \cdot R_{1,q}$	$d_7 t \equiv 1 \pmod{\delta_7}$
$\Gamma(3,p) \wedge \Gamma(2,q)$	$\delta_8 = R_{3,p_i} \cdot R_{2,q}$	$d_8 t \equiv 1 \pmod{\delta_8}$
$\Gamma(3,p) \wedge \Gamma(3,q)$	$\delta_9 = R_{3,p_i} \cdot R_{31,q}$	$d_9 t \equiv 1 \pmod{\delta_9}$

Tabela 3.1: Chaves de Decodificação

Observação 3.2 *Pelo Lema* 1.9 *os polinômios*

$$x^3 - u_1 x^2 + u_2 x - 1 \ \ e \ \ x^3 - c_1 x^2 + c_2 x - 1$$

têm a mesma ordem. Assim, o usuário (receptor) u_j *poderá selecionar uma chave de decodificação*

$$k_{d,j} = (n_i, d_r)$$

apropriada, de acordo com o polinônio construído pelo texto-cifrado

$$\mathbf{c} = (c_1, c_2)\,.$$

A Tabela 3.1 *dá a construção destas chaves de decodificação.*

Exemplo 3.2 *A correspondência entre o alfabeto* $\mathbb{A}$ *e números inteiros é dada pela Tabela* 2.1. *Sejam* $p = 5$, $q = 7$, $n = pq = 35$ *e* $t = 5$ *escolhido convenientemente. Assim, para codificar o texto-original*

$$\text{“}ASBF\text{”}$$

dividimos em blocos de dois símbolos, com correspondência numérica

$$\begin{array}{cc} AS & BF \\ \updownarrow & \updownarrow \\ 18 & 32 \end{array}$$

o usuário u_i *com chave de codificação*

$$\begin{aligned} k_{c,i} &= (n_i, t_i) \\ &= (35, 5) \end{aligned}$$

calcula

$$c_1 = s_5(18, 32) = 33 \ \ e \ \ c_2 = s_{-5}(18, 32) = 12.$$

Logo, o texto-cifrado é o par

$$\mathbf{c} = (c_1, c_2) = (33, 12)$$

onde

$$\begin{aligned} c_1 &\equiv 33 \equiv 1 \cdot 27 + 6 \pmod{35} \\ c_2 &\equiv 12 \equiv 0 \cdot 27 + 12 \pmod{35}. \end{aligned}$$

Portanto, o usuário u_i *envia para o usuário* u_j*, o texto-cifrado*

$$\text{“}BGAM\text{”}.$$

Após recuperar $\mathbf{c} = (33, 12)$*, como obter a chave de decodificação? Para* $p = 5$ *e*

$$\begin{aligned} f(x) &= x^3 - 33x^2 + 12x - 1 \\ &\equiv x^3 - 3x^2 + 2x - 1 \pmod{5} \\ &= (x^2 + 0x + 2)(x - 3) \pmod{5}, \end{aligned}$$

o usuário u_j *calcula*

$$C(3, 2) = 0, D(3, 2) = 4 \ \ e \ \ \Delta(3, 2) = 3.$$

Como $\Delta(3, 2) \neq 0$ *e o símbolo de Legendre*

$$\left(\frac{\Delta(3, 2)}{5}\right) = -1$$

temos a função lógica

$$\Gamma(2, 5).$$

Do mesmo modo para $q = 7$ *e*

$$\begin{aligned} f(x) &= x^3 - 33x^2 + 12x - 1 \\ &\equiv x^3 - 5x^2 + 5x - 1 \pmod{7} \\ &= (x^2 + 3x + 1)(x - 1) \pmod{7}, \end{aligned}$$

o usuário u_j calcula

$$C(5,5) = 4, D(5,5) = 3 \ \ e \ \ \Delta(5,5) = 5.$$

Como $\Delta(5,5) \neq 0$ e o símbolo de Legendre

$$\left(\frac{\Delta(5,5)}{7}\right) = -1$$

temos a função lógica

$$\Gamma(2,7).$$

Assim, de acordo com a Tabela 3.1*, obtemos a condição*

$$\Gamma(2,5) \wedge \Gamma(2,7)$$

e o multiplicador de peíodo

$$\begin{aligned} \delta_5 &= R_{2,5} \cdot R_{2,7} \\ &= 24 \cdot 48 \\ &= 1.152 \end{aligned}$$

Finalmente, como

$$d_5 \cdot t \equiv 1 \pmod{\delta_5}$$

temos que

$$d_5 \cdot 5 \equiv 1 \pmod{1.152}.$$

Portanto, $d_5 = 461$. Agora, com a chave de decodificação

$$k_{d,j} = (35, 461)$$

o usuário u_j calcula

$$\begin{aligned} u_1 &= s_{461}(33,12) = s_5(33,12) = 18, \\ u_2 &= s_{-461}(33,12) = s_3(33,12) = 32 \end{aligned}$$

e recupera a mensagem original

$$\begin{aligned} \mathbf{u} &= (u_1, u_2) \\ &= (18, 32). \end{aligned}$$

Portanto, o texto original é

.

Observação 3.3 *A segurança deste sistema está baseado na dificuldade de fatorar um grande inteiro composto, ou seja, estima-se que para fatorar um número de* 500 *dígitos exige aproximadamente* 10^{25} *anos.*

Referências Bibliográficas

[1] Bhattacharya, P. B., Jain, S. K. e Nagpaul, S. R., *Basic Abstract Algebra*. Cambridge, New York, 1995.

[2] Diffie, W. and Hellman, M. E., "New Directions in Cryptography," *IEEE Trans. Infor. Theory*, vol IT-22, pp 644 – 654, Nov. 1976.

[3] ElGamal, T., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. Infor. Theory*, vol IT-31, pp 469 – 472, jul. 1985.

[4] Garcia, A. L. e Lequain, Y., *Álgebra: Um Curso de Introdução*. IMPA, Rio de Janeiro, 1988.

[5] Golomb, S. W., *Shift Register Sequences.* Laguna Hills, CA Aergean Park, 1982.

[6] Gong, G. and Harn, L. "Public-Key Cryptosystems Based on Cubic Finite Field Extentions," *IEEE Trans. Infor. Theory*, vol IT-45, pp 2601 – 2605, Nov. 1999.

[7] Koblitz, N., *A Course in Number Theory and Cryptography.* Springer, New York, 1994.

[8] Lidl, R. and Pilz, G., *Applied Abstract Algebra.* Springer, New York, 1998.

[9] Lidl, R. and Niederreiter, H., *Finite Fields.* in Encyclopedia of Mathematics and Its Applications, vol. 20, 1983

[10] Rédei, L., *Algebra.* U.K.: Pergamon, London, 1967.

[11] Rivest, R., Shamir, A. and Adleman, L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Commun. ACM*, vol. 21, pp. 120 – 126, 1978.

[12] Rotman, J. J., *Galois Theory.* Springer, New York, 1998.

[13] Sidki, S., *Introdução à Teoria dos Números*. IMPA, Rio de Janeiro, 1975.

[14] Silva, A. A., *Notas de Aulas*, Depto de Matemática, UFPB - Campus I.