UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
DEPARTAMENTO DE MATEMÁTICA

Teoria dos Números e Criptografia

Relatório Final

José Laudelino de Menezes Neto

Antônio de Andrade e Silva
Orientador

agosto de 2005

Sumário

1 Introdução **1**

2 Objetivo **2**

3 Algoritmos Fundamentais **3**
3.1 Algoritmo da Divisão 3
3.2 Representação de um número em uma base qualquer 4
3.3 Algoritmo Euclidiano 5
3.4 Equações Diofantinas 6

4 Fatoração Única **8**

5 Congruência de Números Inteiros **10**
5.1 Congruências Lineares 11
5.2 Sistema de Congruências 12

6 Corpos Finitos **15**
6.1 Corpos 15
6.2 Corpos Finitos 16
6.3 O conjunto $\mathbb{Z}_n$ 16
6.4 A função ϕ de Euler 16

7 Criptografia **18**
7.1 Outros Métodos para Criptografar 20
7.2 Quebrando o Código 21
7.3 Tornando seu Código mais Seguro 21

8 Resíduos Quadráticos e Lei da Reciprocidade Quadrática **22**

9 Logaritmo Discreto e o Problema da Mochila **25**
9.1 Raízes da Unidade 25
9.2 Logaritmo Discreto 26
9.3 Algoritmo para determinar o logaritmo discreto em um corpo finito . 26
9.4 Problema da Mochila 28

10 Criptografia RSA **31**
10.1 Conceitos Básicos 31
10.2 Mecânica do Sistema Assimétrico 31
10.3 O Sistema RSA 32
10.4 Assinatura 33

11 Conclusão **35**

Referências Bibliográficas **36**

Capítulo 1

Introdução

O uso de métodos criptográficos remonta à época egípcia, estando presente na escrita hierográfica. O imperador romano Júlio César usou um modelo criptográfico baseado na substituição de letras do alfabeto denominado C3, para enviar suas mensagens a Marco Túlio, sobre planos de batalha.

Durante muito tempo a criptografia foi usada, basicamente para informar estratégias militares, espionagens e outros assuntos que envolviam segredos militares. Foi tão importante o trabalho criptográfico desenvolvido na Segunda Guerra Mundial, que formou a base da ciência da computação moderna. Atualmente, além deste tipo de uso, ela também tem merecido a atenção de pesquisadores, quanto a seu uso comercial, usada basicamente para se proteger transmissões de dados entre computadores; neste uso se enquadra, por exemplo, as comunicações via Internet, como também as transmissões bancárias, que envolvem transferências entre contas correntes, além de outras atividades típicas do sistema bancário. Valendo ressaltar, que, até recentemente os bancos se preocuparam em expandir o sistema, incorporando maior número de serviços e clientes, passando hoje a investir mais em segurança onde processos criptográficos são necessários.

Dentre os vários sistemas criptográficos, um dos mais importantes é o sistema RSA, que usa fortemente a Teoria dos Números. Este sistema foi criado por Rivest, Shamir e Adleman em 1978.

O estudo deste processo será o objeto principal do projeto, que abordará também os sistemas: *Cripto-sistemas com Chave Pública baseada em Extensões Cúbicas.*

Capítulo 2

Objetivo

No decorrer deste trabalho iremos estudar e analisar alguns tipos específicos de métodos criptográficos com chave pública com o objetivo de desenvolver um algoritmo de codificação do tipo **RSA** (Rivest, Shamir e Adleman).

O estudo desses sistemas irá requerer o uso de várias ferramentas matemáticas tais como: *Teoria dos Números, Corpos Finitos, Resíduos Quadráticos, Problemas de Primalidade e Fatoração.*

O estudo destes assuntos poderá servir de base ao aluno para que este possa iniciar seus estudos na pós-graduação em Matemática Pura, Matemática Aplicada, Engenharia Elétrica, Ciência da Computação etc.

Capítulo 3

Algoritmos Fundamentais

Neste capítulo revisaremos alguns algoritmos e resultados fundamentais que serão úteis nos capítulos subsequentes.

3.1 Algoritmo da Divisão

Dados dois inteiros a e b, ao dividirmos a por b, iremos obter um quociente $q \in \mathbb{Z}$ e um resto $r \in \mathbb{Z}_+^*$. Formalmente:

Teorema 3.1 *Dados $a, b \in \mathbb{Z}$ com $b > 0$, então existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = qb + r, \text{ onde } 0 \leq r < b.$$

Corolário 3.2 (Algoritmo da Divisão) *Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, então existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = qb + r, \text{ onde } 0 \leq r < |b|$$

Exemplo 3.3 *Dados $a = 54$ e $b = 7$, então, tomamos $q = 7$ e $r = 5$, daí*

$$54 = 7 \cdot 7 + 5.$$

Exemplo 3.4 *Dados $a = 4967$ e $b = 597$, então, tomamos $q = 8$ e $r = 191$, daí*

$$4967 = 8 \cdot 597 + 191.$$

Sejam $a, b \in \mathbb{Z}$. Dizemos que a é divisível por b, ou b divide a, ou a é um múltiplo de b, quando existe $q \in \mathbb{Z}$ tal que

$$a = qb.$$

Notação: $b \mid a$.

Caso contrário, dizemos que b não divide a. Notação: $b \nmid a$.

Exemplo 3.5 $4 \mid 8$, *pois*

$$8 = 2 \cdot 4.$$

Esta relação de divisibilidade é uma relação de equivalência, ou seja, dados $a, b, c \in \mathbb{Z}^*$, então as três condições a seguir são satisfeitas

1. $a \mid a$ para todo $a \in \mathbb{Z}^*$
2. Se $a \mid b$ e $b \mid a$, então $a = \pm b$.
3. Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Teorema 3.6 *Sejam $a, b, c \in \mathbb{Z}^*$, então*

1. $\pm 1 \mid a$ *e* $\pm a \mid a$.
2. $a \mid 1 \Leftrightarrow a = \pm 1$.
3. $a \mid b \Leftrightarrow ac \mid bc$.
4. *Se* $c \mid a$ *e* $c \mid b$, *então* $c \mid ax + by$, $\forall x, y \in \mathbb{Z}$.

3.2 Representação de um número em uma base qualquer

Teorema 3.7 *Sejam $a, b \in \mathbb{Z}$ com $b > 1$. Então existem únicos inteiros $n, r_i \in \mathbb{Z}_+$ tais que*

$$a = b^n r_n + b^{n-1} r_{n-1} + \ldots + b^2 r_2 + b^1 r_1 + b^0 r_0 = (r_n r_{n-1} \ldots r_2 r_1 r_0)_b,$$

onde $r_i \in \{0, 1, 2, \ldots, b-1\}, \forall i = 0, 1, \ldots, n$ e $n = \lfloor \log_b a \rfloor$.

Dizemos que $a = (r_n r_{n-1} \ldots r_2 r_1 r_0)_b$ é a representação do inteiro a na base b e que $n + 1$ é o número de dígitos na base b.

A prova do Teorema 3.7 nos dá um Algortimo prático de como escrever um número $a \in \mathbb{Z}$ em qualquer outra base $b > 1$.

Vejamos o Algoritmo:

Pelo Algoritmo da Divisão, Corolário 3.2, sabemos que existem $r_i, q_i \in \mathbb{Z}$ $(i = 0, 1, \ldots, n)$ tais que

$$\begin{array}{ccccc}
a & = & q_0 b + r_0, & & 0 \leq r_0 < b \\
q_0 & = & q_1 b + r_1, & & 0 \leq r_1 < b \\
q_1 & = & q_2 b + r_2, & & 0 \leq r_2 < b \\
\vdots & \vdots & \vdots & & \vdots \\
q_{n-2} & = & q_{n-1} b + r_{n-1}, & & 0 \leq r_{n-1} < b \\
q_{n-1} & = & 0 \cdot b + r_n, & & 0 \leq r_n < b
\end{array}$$

Daí tiramos os restos r_i $(i = 0, 1, \ldots, n)$, os quais são os dígitos de a na base b e, assim, podemos escrever $a = (r_n r_{n-1} \ldots r_2 r_1 r_0)_b$.

Exemplo 3.8 *Vamos escrever o número* 382 *na base* 3.

Solução: Pelo Algoritmo da Divisão:

$$\begin{array}{rcl}
382 & = & 127 \cdot 3 + 1 \\
127 & = & 42 \cdot 3 + 1 \\
42 & = & 14 \cdot 3 + 0 \\
14 & = & 4 \cdot 3 + 2 \\
4 & = & 1 \cdot 3 + 1 \\
1 & = & 0 \cdot 3 + 1
\end{array}$$

Daí, $r_5 = 1, r_4 = 1, r_3 = 2, r_2 = 0, r_1 = 1$ e $r_0 = 1$. Logo,

$$382 = 3^5 \cdot 1 + 3^4 \cdot 1 + 3^3 \cdot 2 + 3^2 \cdot 0 + 3^1 \cdot 1 + 3^0 \cdot 1 = (112011)_3.$$

3.3 Algoritmo Euclidiano

O Algoritmo Euclidiano é um algoritmo utilizado para determinar o Máximo Divisor Comum (MDC) de dois números. Antes, veremos a definição de MDC e alguns resultados básicos para, enfim, enunciarmos o Algoritmo Euclidiano.

Definição 3.9 (Máximo Divisor Comum) *Dados $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$, então existe um inteiro positivo $d = mdc(a, b)$, denominado máximo divisor comum de a e b, tal que*

1. *$d \mid a$ e $d \mid b$.*
2. *Se existir $c \in \mathbb{Z}^*$ tal que $c \mid a$ e $c \mid b$, então $c \mid d$.*

Proposição 3.10 *Sejam $a, b \in \mathbb{Z}$. Se $mdc(a, b)$ existe, então $mdc(a, b)$ é único.*

Teorema 3.11 *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Se $mdc(a, b) = d$, então existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$.*

Teorema 3.12 *Sejam $a, b \in \mathbb{Z}^*$. $mdc(a, b) = 1$ se, e somente se, existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$.*

Lema 3.13 *Sejam $a, b, c \in \mathbb{Z}^*$. Então, $mdc(ca, cb) = |c|mdc(a, b)$.*

Lema 3.14 *Sejam $a, b \in \mathbb{Z}$. Se $a = qb + r$ com $q, r \in \mathbb{Z}$ e $0 \leq r < b$, então $mdc(a, b) = mdc(b, r)$.*

Lema 3.15 (Euclides) *Sejam $a, b, c \in \mathbb{Z}^*$. Se $mdc(a, c) = 1$ e $c \mid ab$, então $c \mid b$.*

Agora, estamos em condições de enunciar o Algoritmo Euclidiano.

Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Se um dos dois for zero, digamos $b = 0$, então $mdc(a, b) = a$. Agora, se $a \neq 0$ e $b \neq 0$, então, pelo Algoritmo da Divisão, existem q_1, r_1 tais que

$$a = q_1 b + r_1, \text{ onde } 0 \leq r_1 < b.$$

Se $r_1 = 0$, então $mdc(a, b) = b$. Caso contrário, $r_1 \neq 0$, então existem $q_2, r_2 \in \mathbb{Z}$ tais que

$$b = q_2 r_1 + r_2, \text{ onde } 0 \leq r_2 < r_1.$$

Se $r_2 = 0$, então, pelo Lema 3.14, $mdc(a, b) = mdc(b, r_1) = r_1$. Caso contrário, $r_2 \neq 0$, então repete-se o processo até que um dos r_i seja igual a zero, digamos $r_{n+1} = 0$, e, finalmente, concluiremos que

$$mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = \ldots = mdc(r_{n-1}, r_n) = r_n.$$

Note que, necessariamete, um dos restos deverá ser zero, no caso $r_{n+1} = 0$, pois uma sequência decrescente de números inteiros positivos

$$r_1 > r_2 > r_3 > \ldots > r_n > 0$$

não pode ser infinita por conta do seguinte axioma

Axioma 3.16 (Axioma da Boa Ordenação) *Todo subconjunto não vazio de* $\mathbb{N}$ *contém menor elemento.*

Pelo Algoritmo Euclidiano também é possível determinar o $x \in \mathbb{Z}$ e o $y \in \mathbb{Z}$ citados pelo Teorema 3.11.

Exemplo 3.17 *Determinar o máximo divisor comum de* 87 *e* 39 *e* $x, y \in \mathbb{Z}$ *tais que* $87x + 39y = mdc(87, 39)$.

Solução: Primeiro vamos determinar o $mdc(87, 39)$. Utilizando Algoritmo da Divisão

$$\begin{aligned} 87 &= 2 \cdot 39 + 9 && (3.1)\\ 39 &= 4 \cdot 9 + 3 && (3.2)\\ 9 &= 3 \cdot 3 + 0 && (3.3) \end{aligned}$$

Da equação 3.3 podemos concluir pelo Algoritmo da Euclidiano que
$mdc(87, 39) = 3$.
Como $mdc(87, 39) = 3$, então, determinaremos $x, y \in \mathbb{Z}$ tais que $87x + 39y = 3$. Da equação 3.2 temos

$$39 + (-4) \cdot 9 = 3. \tag{3.4}$$

Pela equação 3.1 temos

$$87 + (-2) \cdot 39 = 9. \tag{3.5}$$

De (3.4) e (3.5) temos

$$\begin{aligned} 3 &= 39 + (-4) \cdot \overbrace{[87 + (-2) \cdot 39]}^{=9}\\ 3 &= 39 + (-4) \cdot 87 + (-4) \cdot (-2) \cdot 39\\ 3 &= (-4) \cdot 87 + (8 + 1) \cdot 39\\ 3 &= (-4) \cdot 87 + 9 \cdot 39 \end{aligned}$$

Logo, $x = -4$ e $y = 9$.

3.4 Equações Diofantinas

Uma equação algébrica com coeficientes constantes inteiros é chamada de Equação Diofantina se suas soluções são números inteiros ou racionais. Vamos nos restringir a Equações Diofantinas da forma

$$ax + by = c \text{ com } a, b, c \in \mathbb{Z}. \tag{3.6}$$

Este tipo de Equação Diofantina, equação 3.6, irá nos auxiliar na resolução de congruências lineares. Para determinarmos uma solução para esta Equação Diofantina utilizamos o Algoritmo Euclidiano e o Teorema 3.11.

Proposição 3.18 *Sejam* $a, b, c \in \mathbb{Z}^*$ *e* $mdc(a, b) = d$. *Então, as seguintes afirmações são verdadeiras:*

1. *A equação $ax + by = c$ tem solução em $\mathbb{Z}$ se, e somente se, d divide c;*
2. *Se $x_0, y_0 \in \mathbb{Z}$ é uma solução particular da equação $ax + by = c$, então,*

$$x = x_0 + k\frac{b}{d} \quad e \quad y = y_0 - k\frac{a}{d}, \forall k \in \mathbb{Z}$$

   também o é;

3. *Se $d = 1$ e $c \geq ab$, então, existem $x, y \in \mathbb{Z}_+$ tais que $ax + by = c$.*

Exemplo 3.19 *Determinar, se existir, a solução geral em $\mathbb{Z}$ da Equação Diofantina $87x + 39y = 105$.*

Solução: Pelo Exemplo 3.17 sabemos que $mdc(87, 39) = 3$ e $3 \mid 105$. Logo, pelo ítem 1 da Proposição 3.18, a Equação Diofantina $87x + 39y = 105$ tem solução em $\mathbb{Z}$. Também, pelo Exemplo 3.17, sabemos que

$$87 \cdot (-4) + 39 \cdot 9 = 3. \tag{3.7}$$

Como $105 = 35 \cdot 3$, então, multiplicando (3.7) por 35 encontramos

$$87 \cdot (-4) \cdot 35 + 39 \cdot 9 \cdot 35 = 3 \cdot 35 \Rightarrow 87 \cdot (-140) + 39 \cdot 315 = 105$$

daí, $x_0 = -140$ e $y_0 = 315$ é uma solução particular e, portanto, pelo ítem 2 da Proposição 3.18,

$$x = -140 + k13 \quad \text{e} \quad y = 315 - k29, \forall k \in \mathbb{Z}$$

é a solução geral da Equação Diofantina $87x + 39y = 105$.

Capítulo 4

Fatoração Única

A fatoração única nada mais é que a decomposição de um número inteiro em todos os seus fatores primos. O Teorema Fundamental da Arítimética, que será aprensentado neste capítulo, garante a unicidade desta fatorização. Esta fatoração será importante quando tratarmos da Função de Euler.

Antes de enunciarmos o referido Teorema, vejamos algumas definições e resultados que são úteis para a compreensão do mesmo.

Definição 4.1 *Um número primo é um inteiro $p \neq \pm 1$ o qual não possui divisores além de ± 1 e $\pm p$, ou seja, p possui apenas os divisores triviais ± 1 e $\pm p$.*

Definição 4.2 *Um número inteiro é chamado composto ou redutível se tiver ao menos um divisor não trivial.*

Teorema 4.3 *Se $a \in \mathbb{Z}$, com $|a| > 1$, então existe um número primo p que divide a.*

Teorema 4.4 *Seja $a \in \mathbb{Z}$, com $|a| > 1$, um número composto. Então, a contém um divisor primo p tal que $p \leq \sqrt{|a|}$.*

Lema 4.5 *Sejam $a, b \in \mathbb{Z}^*$. Se p é um número primo e $p|ab$, então $p|a$ ou $p|b$.*

Corolário 4.6 *Se p é um número primo e $p|p_1 p_2 \dots p_n$, onde $p_1, p_2, \dots, p_n$ são números primos, então $p = p_i$ para algum $i = 1, 2, \dots, n$.*

Teorema 4.7 (Teorema Fundamental da Aritmética) *Todo $a \in \mathbb{Z}\backslash\{-1, 0, 1\}$ pode ser escrito de modo único, a menos da ordem dos fatores, na forma*

$$a = up_1 p_2 \dots p_n,$$

onde $u = \pm 1$ e $p_1, p_2, \dots, p_n$ são números primos.

Corolário 4.8 *Todo $a \in \mathbb{Z}\backslash\{-1, 0, 1\}$ pode ser escrito de modo único na forma*

$$a = up_1^{r_1} p_2^{r_2} \dots p_n^{r_n},$$

onde $u = \pm 1$, $p_1 < p_2 < \dots < p_n$ são números primos e $r_i \in \mathbb{N} \cup \{0\}$ $i = 1, 2, \dots, n$.

O Teorema Fundamental da Aritmética nos garante a existência de uma fatorização canônica para qualquer inteiro a diferente de -1, 0 e 1, porém o problema de encontrá-la pode ser bastante trabalhosa. Uma maneira direta de proceder é verificar, braçalmente ou pelo uso de um computador, a divisibilidade de a por inteiros b menores do que a. Pelo Teorema 4.4, é suficiente verificar a divisibilidade de a pelos primos menores ou iguais a $\sqrt{|a|}$ (Sidki, 1975).

Capítulo 5

Congruência de Números Inteiros

Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Dizemos que a é congruente a b módulo n se $a - b$ é divisível por n, em símbolos

$$a \equiv b \,(\text{mod } n)\,.$$

Em outras palavas, a é congruente a b módulo n, $a \equiv b \,(\text{mod } n)$, se

$$a - b = nq, \text{ com } q \in \mathbb{Z}.$$

Caso contrário, n não dividir $a-b$, então dizemos que a não é congruente a b módulo n, $a \not\equiv b \,(\text{mod } n)$.

A relação de congruência é uma relação de equivalência, ou seja, valem as seguintes afirmações

1. $a \equiv a \,(\text{mod } n)$ para todo $a \in \mathbb{Z}$.
2. Se $a \equiv b \,(\text{mod } n)$, então $b \equiv a \,(\text{mod } n)$.
3. Se $a \equiv b \,(\text{mod } n)$ e $b \equiv c \,(\text{mod } n)$, então $a \equiv c \,(\text{mod } n)$.

Teorema 5.1 *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então, $a \equiv b \,(mod\ n)$ se, e somente se, a e b possuem o mesmo resto quando divididos por n.*

Teorema 5.2 *Sejam $a, b, c, d, x \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então, as seguintes afirmações são verdadeiras:*

1. *Se $a \equiv b \,(mod\ n)$ e $c \equiv d \,(mod\ n)$, então*

$$a + c \equiv b + d \,(mod\ n) \quad e \quad ac \equiv bd \,(mod\ n)\,.$$

2. *Se $a \equiv b \,(mod\ n)$, então $ax \equiv bx \,(mod\ n)$.*
3. *Se $a \equiv b \,(mod\ n)$ e $c \equiv d \,(mod\ n)$, então*

$$ax \equiv c \,(mod\ n) \Leftrightarrow bx \equiv d \,(mod\ n)\,.$$

4. *Se $a \equiv b \,(mod\ n)$, então $a^k \equiv b^k \,(mod\ n)\,, \forall k \in \mathbb{N}$.*
5. *Se $ac \equiv bc \,(mod\ n)$ e $mdc(c, n) = 1$, então $a \equiv b \,(mod\ n)$.*

5.1 Congruências Lineares

Uma Congruência Linear é uma congruencia da forma

$$ax \equiv b \,(\text{mod } n) \tag{5.1}$$

com $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Note que a congruência linear (5.1) nem sempre tem solução em $\mathbb{Z}$; por exemplo, a congruencia linear

$$3x \equiv 4 \,(\text{mod } 3) \tag{5.2}$$

não tem solução em $\mathbb{Z}$ (Silva). De fato, caso a congruência (5.2) tivesse solução, então teríamos que

$$3x - 4 = 3q, \quad \text{com} \quad q, x \in \mathbb{Z}$$

que é equivalente a

$$3x - 3q = 4, \quad \text{com} \quad q, x \in \mathbb{Z}.$$

Perceba que $3x - 3q = 4$ é uma Equação Diofantina e $mdc(3, -3) = 3$. Como $3 = mdc(3, -3)$ não divide 4, então, pelo ítem 1 da Proposição 3.18, a Equação Diofantina $3x - 3q = 4$ não tem solução em $\mathbb{Z}$ e, por conseguinte, a congruência linear (5.2) não tem solução em $\mathbb{Z}$. Destas observações podemos deduzir o seguinte Teorema:

Teorema 5.3 *Sejam $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ e $mdc(a, n) = d$. Então, a congruência linear $ax \equiv b \,(mod\ n)$ tem solução em $\mathbb{Z}$ se, e somente se, d divide b.*

Teorema 5.4 *Sejam $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ e $mdc(a, n) = d$. Se $x_0 \in \mathbb{Z}$ é uma solução particular da congruência linear $ax \equiv b \,(mod\ n)$, então*

$$x = x_0 + k\frac{n}{d}, k \in \mathbb{Z}$$

é a solução geral da congruência linear $ax \equiv b \,(mod\ n)$.

Vejamos dois exemplos:

Exemplo 5.5 *Determinar, se existir, a solução geral em $\mathbb{Z}$ da congruência linear*

$$87x \equiv 105 \,(mod\ 39)\,.$$

Solução: Pelo Exemplo 3.17, temos que $mdc(87, 39) = 3$ e que $3 \mid 105$, então, pelo Teorema 5.3, a congruência linear $87x \equiv 105 \,(\text{mod } 39)$ tem solução em $\mathbb{Z}$.

Sabemos que

$$\begin{aligned} & 87x \equiv 105 \,(\text{mod } 39) && \Leftrightarrow \\ \Leftrightarrow \quad & 87x - 105 = 39q, q \in \mathbb{Z} && \Leftrightarrow \\ \Leftrightarrow \quad & 87x - 39q = 105. && (5.3) \end{aligned}$$

Note que a equação (5.3) é semelhante a Equação Diofantina $87x + 39y = 105$ encontrada no Exemplo 3.19. Então, pelo Exemplo 3.19, temos $x_0 = -140$ e $q_0 = -315 \Rightarrow 87 \cdot (-140) - 39 \cdot (-315) = 105 \Rightarrow 87 \cdot (-140) \equiv 105 \,(\text{mod } 39)$. Logo, $x_0 = -140$ é uma solução particular e, portanto, pelo Teorema 5.4,

$$x = -140 + 13k, k \in \mathbb{Z}$$

é a solução geral da congruência linear $87x \equiv 105 \,(\text{mod } 39)$.

Exemplo 5.6 *Determinar, se existir, a solução geral em* $\mathbb{Z}$ *da congruência linear*

$$26x \equiv 25\,(mod\ 13)\,.$$

Solução: Primeiro, vamos determinar $mdc(26, 13)$. Sabemos que $26 = 2 \cdot 13 + 0$, então, pelo Algoritmo Euclidiano, $mdc(26, 13) = 13$. Agora, iremos verificar se a congruência linear $26x \equiv 25\,(\text{mod } 13)$ possui solução em $\mathbb{Z}$. Como $13 = mdc(26, 13)$ e $13 \nmid 25$, logo, pelo Teorema 5.3, a congruência linear $26x \equiv 25\,(\text{mod } 13)$ não tem solução em $\mathbb{Z}$.

5.2 Sistema de Congruências

Sejam $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k, n_1, n_2, \ldots, n_k \in \mathbb{Z}$ e $k \in \mathbb{N}$. Um sistema de congruências é um sistema da forma

$$\begin{cases} a_1x \equiv b_1\,(\text{mod } n_1) \\ a_2x \equiv b_2\,(\text{mod } n_2) \\ \qquad\vdots \\ a_kx \equiv b_k\,(\text{mod } n_k) \end{cases}$$

e nesta seção estamos interessados em encontrar a solução geral para este sistema.

Vejamos um exemplo:

Exemplo 5.7

$$\begin{cases} x \equiv 1\,(mod\ 3) \\ x \equiv 2\,(mod\ 5) \\ x \equiv 3\,(mod\ 7) \end{cases}$$

Solução: Sabemos que a solução geral da primeira congruência é

$$x = 1 + 3y, \forall y \in \mathbb{Z}$$

Substituindo na segunda congruência, obtemos

$$1 + 3y \equiv 2\,(\text{mod } 5) \Leftrightarrow 3y \equiv 1\,(\text{mod } 5)\,,$$

cuja solução geral é

$$y = 2 + 5z, \forall z \in \mathbb{Z}.$$

Logo,

$$\begin{aligned} x &= 1 + 3y \\ &= 1 + 3(2 + 5z) \\ &= 7 + 15z, \forall z \in \mathbb{Z} \end{aligned}$$

é solução simultânea das duas congruências. Finalmente, substituindo na terceira congruência, obtemos

$$7 + 15z \equiv 3\,(\text{mod } 7) \Leftrightarrow 15z \equiv 3\,(\text{mod } 7)\,,$$

cuja solução geral é

$$z = 3 + 7k, \forall k \in \mathbb{Z}.$$

Portanto,

$$\begin{aligned} x &= 7 + 15z \\ &= 7 + 15(3 + 7k) \\ &= 52 + 105k, \forall k \in \mathbb{Z} \end{aligned}$$

é a solução geral do sistema e $x_0 = 52$ é uma solução particular (Silva).

A demonstração do Teorema Chinês dos Restos nos dá um algoritmo que auxilia para determinarmos uma solução particular.

Teorema 5.8 (Teorema Chinês dos Restos) *Sejam $b_1, \ldots, b_k \in \mathbb{Z}$ e $n_1, \ldots, n_k \in \mathbb{N}$ tais que $mdc(n_i, n_j) = 1$ com $i \neq j$. Então, o sistema de congruências*

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

tem uma única solução x_0 com $1 \leq x_0 < n$, onde $n = n_1 n_2 \ldots n_k$. Além disso,

$$S = \{x_0 + kn; k \in \mathbb{Z}\}$$

é o conjunto de todas as soluções deste sistema.

Demonstração: É claro que

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

para todo $i = 1, 2, \ldots, k$. Logo, pelos Teoremas 5.3 e 5.4, para cada i existe $r_i \in \mathbb{Z}$ tal que

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

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

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

Assim, tomando

$$x_0 = \sum_{i=1}^{k} \frac{n}{n_i} r_i b_i$$

obtemos que

$$x_0 \equiv b_i \,(\text{mod } n_i)\,, \forall i = 1, 2, \ldots, k;$$

isto é, x_0 é uma solução do sistema de congruências.

Sejam $x_1, x_2 \in \mathbb{Z}$ duas soluções do sistema de congruências com

$$1 \leq x_1 \leq x_2 < n.$$

Então,

$$x_1 \equiv x_2 \,(\text{mod } n_i)\,, \forall i = 1, 2, \ldots, k$$

e, portanto, $x_1 \equiv x_2 \,(\text{mod } n)$, isto é, $n \mid (x_1 - x_2)$. Como $1 \leq x_1 - x_2 < n$ temos que $x_1 = x_2$. ■

Iremos resolver, novamente, o Exemplo 5.7 utilizando o Teorema Chinês dos Restos.

Exemplo 5.9

$$\begin{cases} x \equiv 1\,(mod\ 3) \\ x \equiv 2\,(mod\ 5) \\ x \equiv 3\,(mod\ 7) \end{cases}$$

Solução utilizando o Teorema Chinês dos Restos: Neste caso temos $k = 3, b_1 = 1, b_2 = 2, b_3 = 3, n_1 = 3, n_2 = 5, n_3 = 7$ e

$$n = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 5 \cdot 7 \cdot = 105.$$

Note que $mdc(3, 5) = mdc(3, 7) = mdc(5, 7) = 1$, então, pelo Teorema Chinês dos Restos, este sistema de congruências tem uma única solução x_0 com $1 < x_0 \leq 105$. Como

$$mdc(\frac{105}{3}, 3) = mdc(35, 3) = 1,$$

temos, pelo Algoritmo Euclidiano, que $3 \cdot 12 + (-1) \cdot 35 = 1$, isto é

$$(-1) \cdot 35 \equiv 1 \,(\text{mod } 3)\,.$$

Assim, podemos escolher $r_1 = -1$. De modo análogo, temos $r_2 = 1$ e $r_3 = 1$. Logo,

$$\begin{aligned} x_0 &= \sum_{i=1}^{k} \frac{n}{n_i} r_i b_i \\ &= \frac{n}{n_1} \cdot r_1 \cdot b_1 + \frac{n}{n_2} \cdot r_2 \cdot b_2 + \frac{n}{n_3} \cdot r_3 \cdot b_3 \\ &= 35 \cdot (-1) \cdot 1 + 21 \cdot 1 \cdot 2 + 15 \cdot 1 \cdot 3 \\ &= -35 + 42 + 45 \\ &= -35 + 87 \\ &= 52. \end{aligned}$$

Portanto, $x_0 = 52$ é a solução particular e

$$S = \{x_0 + nk; k \in \mathbb{Z}\} = \{52 + 105k; k \in \mathbb{Z}\}$$

é o conjunto de todas as soluções deste sistema. Comparando com o resultado obtido no Exemplo 5.7, vemos que a solução é a mesma.

Capítulo 6

Corpos Finitos

6.1 Corpos

A definição de corpo abaixo é encontrada em Lima páginas 49 e 50.

Um *corpo* é um conjunto K, munido de duas operações, as quais iremos chamar de *adição* e *multiplicação*, que satisfazem a certas condições, chamadas os *axiomas de corpo*, especificadas abaixo.

A adição faz corresponder a cada par de elementos $x, y \in K$ sua *soma* $x+y \in K$, enquanto a multiplicação associa a esses elementos o seu produto $x \cdot y \in K$. Os axiomas de corpo são os seguintes:

A. Axiomas da adição

A1. *Associatividade* – quaisquer que sejam $x, y, z \in K$, tem-se

$$(x + y) + z = x + (y + z).$$

A2. *Comutatividade* – quaisquer que sejam $x, y \in K$, tem-se

$$x + y = y + x.$$

A3. *Elemento neutro* – existe $0 \in K$ tal que $x + 0 = x$, seja qual for $x \in K$. O elemento 0 chama-se **zero**.

A4. *Simétrico* – todo elemento $x \in K$ possui um simétrico $-x \in K$ tal que

$$x + (-x) = 0.$$

B. Axiomas da multiplicação

M1. *Associatividade* – dados quaisquer $x, y, z \in K$, tem-se

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

M2. *Comutatividade* – sejam quais forem $x, y \in K$, vale

$$x \cdot y = y \cdot x.$$

M3. *Elemento neutro* – existe $1 \in K$ tal que $1 \neq 0$ e $x \cdot 1 = x$, qualquer que seja $x \in K$. O elemento 1 chama-se **um**.

M4. *Inverso multiplicativo* – todo $x \neq 0$ em K possui um inverso x^{-1} tal que

$$x \cdot x^1 = 1.$$

D. Axioma da distributividade. Dados $x, y, z \in K$, tem-se

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

6.2 Corpos Finitos

Um *corpo finito* é um corpo de *ordem finita*, ou seja, com um número finito de elementos, já que a *ordem* nada mais é que o número de elementos de um corpo. A ordem de um corpo finito é sempre um número primo ou a potência de um número primo.

6.3 O conjunto $\mathbb{Z}_n$

O conjunto $\mathbb{Z}_n$ é o conjunto dos restos da divisão de um inteiro qualquer por n. Vejamos o $\mathbb{Z}_5$

$$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\},$$

pois qualquer número inteiro dividido por 5 deixa restos $0, 1, 2, 3$ ou 4.

O conjunto $\mathbb{Z}_n$ também pode ser visto como o conjunto quociente de $\mathbb{Z}$ pela relação de equivalência *congruência módulo* n ("$\equiv \pmod n$"). No $\mathbb{Z}_5$, o $\bar{0}$ é o subconjunto de $\mathbb{Z}$ formado pelos elementos que são equivalentes a 0, $\bar{0}$ é a *classe de equivalência do* 0, ou seja,

$$\begin{aligned} \bar{0} &= \{a \in \mathbb{Z}; a \equiv 0 \pmod 5\} \\ &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}. \end{aligned}$$

Caso n seja um inteiro primo p, então $\mathbb{Z}_p$ é um corpo finito com as operações de $+$ (soma) e $\cdot$ (multiplicação) assim definidas

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

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

6.4 A função ϕ de Euler

Em $\mathbb{Z}_n$, com a operação de multiplicação definida na seção anterior, um número $\bar{a} \in \mathbb{Z}_n^*$ nem sempre terá um inverso multiplicativo, ou seja, não existe $\overline{a^{-1}} \in \mathbb{Z}_n^*$ tal que $\overline{a^{-1}} \cdot \bar{a} = \bar{1}$. Em $\mathbb{Z}_4$, por exemplo, o $\bar{2}$ não possui inverso multiplicativo. Explicamos isto porque a Função ϕ de Euler é o número de elementos inversíveis de $\mathbb{Z}_n$. Por exemplo,

$$\phi(4) = 2,$$

pois em $\mathbb{Z}_4$ os únicos elementos inversíveis são $\bar{1}$ e $\bar{3}$.

Como $\mathbb{Z}_p$, p primo, é um corpo finito e, pela definição de corpo, todos os elementos são inversíveis com exceção do $\bar{0}$, então

$$\phi(p) = p - 1.$$

Vejamos agora um resultado que é útil para determinarmos se um elemento de $\mathbb{Z}_n$ possui inverso multiplicativo.

Teorema 6.1 *Seja $\bar{a} \in \mathbb{Z}_n$. Então, $\bar{a}$ tem inverso multiplicativo em $\mathbb{Z}_n$ se, e somente se, $mdc(a, n) = 1$.*

O teorema a seguir nos mostra algumas propriedades da função ϕ de Euler.

Teorema 6.2 *Sejam $p, m, n, k, r \in \mathbb{N}$, onde p é primo. Então as seguintes afirmações são verdadeiras:*

1. $\phi(p^k) = p^k(1 - \frac{1}{p})$.
2. *Se $mdc(m, n) = 1$, então $\phi(mn) = \phi(m)\phi(n)$.*
3. *Se $n > 1$, então*

$$\phi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}),$$

onde $p_1, p_2, \ldots, p_r$ são primos distintos que dividem n.

Para provar o ítem 3 é necessário utilizar o **Teorema Fundamental da Aritmética**.

Teorema 6.3 (Teorema de Euler) *Sejam $m, n \in \mathbb{N}$ com $mdc(m, n) = 1$. Então,*

$$n^{\phi(m)} \equiv 1 \,(mod\ m)\,.$$

Corolário 6.4 (Teorema de Fermat) *Seja $p \in \mathbb{N}$ um número primo. Então,*

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

Teorema 6.5 *Sejam $a, n \in \mathbb{N}$, com $mdc(a, n) = 1$. Se $r, t \in \mathbb{N}$ são tais que $rt \equiv 1 \,(mod\ \phi(n))$, então*

$$a^{rt} \equiv a \,(mod\ n)\,.$$

Corolário 6.6 *Sejam $n, r, t \in \mathbb{N}$. Se $mdc(t, \phi(n)) = 1$, então a função*

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

é uma correspondência biunívoca com $f^{-1}(x) = x^r$, onde

$$rt \equiv 1 \,(mod\ \phi(n))\,.$$

Capítulo 7

Criptografia

A criptografia é o estudo de métodos para enviar mensagens em códigos, de modo que apenas sistemas autorizados possam decodificar a mensagem.

A mensagem a ser enviada é chamada de **texto-original** e a mensagem codificada é chamada de **texto-cifrado**. Tanto a mensagem original, quanto a codificada, são escritas em um determinado alfabeto $\mathbb{F}$ composto de n símbolos, ou seja,

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

O texto-original e o texto-cifrado são divididos em mensagens unitárias, as quais são divididas em blocos de k símbolos do alfabeto $\mathbb{F}$. Para codificarmos o texto-original, fazemos uso de uma função f, denominada **cripto-sistema**, a qual irá associar cada mensagem unitária **u** do texto-original a uma mensagem unitária **c** do texto-cifrado. A função f deve ser uma bijeção, pois, caso contrário, teríamos um processo irreversível de codificação, ou seja, codificariamos uma mensagem e não teríamos como decodificá-la. Em outras palavras, f é uma função bijetora que irá levar o conjunto $\mathcal{P}$ de todas as possíveis mensagens unitárias do texto-original ao conjunto $\mathcal{C}$ de todas as possíveis mensagens unitárias do texto-cifrado. A inversa de f, f^{-1}, irá fazer o caminho contrário. Veja o diagrama a seguir:

$$\mathcal{P} \underset{f}{\longrightarrow} \mathcal{C} \underset{f^{-1}}{\longrightarrow} \mathcal{P}.$$

Teorema 7.1 *Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}_n$ fixados. Se $mdc(a, n) = 1$, então, a função*

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

é um cripto-sistema.

Vejamos um exemplo para ilustrar tudo o que foi dito acima.

Exemplo 7.2 *Criptografar a mensagem unitária*

"VIVA-A-MATEMATICA"

do texto-original em blocos de 1 *símbolo utilizando o cripto-sistema*

$$f : \mathbb{Z}_{27} \longrightarrow \mathbb{Z}_{27} \text{ dado por } f(x) = 4x + 6.$$

Solução: Primeiro, associamos cada símbolo do nosso alfabeto $\mathbb{F}$ com um número em $\mathbb{Z}_{27}$

$$\begin{array}{ccccccccccccc} \text{A} & \text{B} & \text{C} & \dots & \text{K} & \text{L} & \text{M} & \dots & \text{V} & \text{W} & \text{X} & \text{Y} & \text{Z} & \text{-} \\ \updownarrow & \updownarrow & \updownarrow & \dots & \updownarrow & \updownarrow & \updownarrow & \dots & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & \dots & 10 & 11 & 12 & \dots & 21 & 22 & 23 & 24 & 25 & 26. \end{array}$$

Agora, calculamos

$$f(\text{V}) = f(21) = 9, f(\text{I}) = f(8) = 11, \dots, f(\text{C}) = f(2) = 14 \text{ e } f(\text{A}) = f(0) = 6,$$

que equivale a mensagem "VIVA-A-MATEMATICA". Depois, associamos de volta os valores encontrados com o alfabeto $\mathbb{F}$ e encontramos a mensagem unitária do texto-cifrado

"JLJGCGCAGBWAGBLOG".

Se quisermos descriptografar esta mensagem, devemos determinar a inversa de f, f^{-1}.

A inversa f^{-1} é dada por

$$f^{-1}(x) = a'x + b', \text{ onde } a' = a^{-1} = 4^{-1} \text{ e } b' = -a' \cdot b = (-4^{-1}) \cdot 6.$$

Sabemos, pelo Teorema 6.1, que 4 possui inverso multiplicativo em $\mathbb{Z}_{27}$. Logo, para determinarmos o inverso de 4, $a' = a^{-1} = 4^{-1}$, devemos resolver a seguinte congruência linear

$$4x \equiv 1 \,(\text{mod } 27)\,,$$

que tem solução $x = a' = 4^{-1} = 7$, pois $4 \cdot 7 \equiv 28 \equiv 1 \,(\text{mod } 27)$. Resta determinarmos b'

$$b' = a' \cdot b = (-4^{-1}) \cdot 6 = (-7) \cdot 6 = -42 \equiv 12 \,(\text{mod } 27)\,.$$

Portanto, a inversa de f é

$$f^{-1}(x) = 7x + 12,$$

de fato,

$$f(f^{-1}(x)) = f(7x + 12) = 4 \cdot (7x + 12) + 6 = 28x + 48 + 6 \equiv x + 54 \equiv x \,(\text{mod } 27)\,.$$

Com a inversa em mãos, calculamos

$$f^{-1}(\text{J}) = f^{-1}(9) = 21, f^{-1}(\text{L}) = f^{-1}(11) = 8, \dots$$

$$\dots, f^{-1}(\text{O}) = f^{-1}(14) = 2 \text{ e } f^{-1}(\text{G}) = f^{-1}(6) = 0,$$

que equivale a mensagem "JLJGCGCAGBWAGBLOG". Fazemos a correspondência com os valores encontrados com o nosso alfabeto $\mathbb{F}$ para obtermos a mensagem descriptografada

"VIVA-A-MATEMATICA".

7.1 Outros Métodos para Criptografar

Em geral, podemos criptografar uma mesma mensagem unitária em blocos de k símbolos do texto-original, de um alfabeto $\mathbb{F}$ de n símbolos por inteiros do conjunto

$$\mathbb{Z}_{n^k} = \{0, 1, 2, \ldots, n^k - 1\}$$

do seguinte modo

$$(x_{k-1}, \ldots, x_2, x_1, x_0) \in \mathbb{Z}_n^k \longleftrightarrow x_{k-1}n^{k-1} + \ldots + x_2n^2 + x_1n + x_0 \in \mathbb{Z}_{n^k},$$

onde cada x_i corresponde a um símbolo do alfabeto $\mathbb{F}$.

Uma outra maneira de transmitir mensagens unitárias, com blocos de k símbolos, é fazer cada bloco de k símbolos corresponder a um vetor

$$\mathbf{x} = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{k-1} \end{bmatrix} \in \mathbb{Z}_n^k.$$

Os resultados a seguir serão enunciados para $k = 2$, mas podem ser generalizados para qualquer $k \geq 2, k \in \mathbb{N}$.

Lema 7.3 *Denotaremos por $M_2(\mathbb{Z}_n)$ o conjunto das matrizes 2×2 com entradas em $\mathbb{Z}_n$. Sejam*

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

Então, as seguintes afirmações são equivalentes:

1. *$mdc(n, D) = 1$;*
2. *A tem uma matriz inversa;*
3. *A função*

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

   é uma bijeção;

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

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

Teorema 7.4 *Sejam $n \in \mathbb{N}$,*

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

e $D = det(A)$. Se $mdc(n, D) = 1$, então a função

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

é um cripto-sistema.

7.2 Quebrando o Código

Assim como a criptografia é o estudo de métodos para enviar mensagens em códigos, existe o estudo para desvendar uma mensagem cifrada sem saber como ela foi criptografada, ou seja, o processo de *cripto-análise*. A pessoa não possui nenhum conhecimento de como a mensagem foi criptografada ou de como descriptografá-la, mas, a partir de uma análise minuciosa, irá tentar quebrar o código e descobrir como a mensagem foi criptografada e, deste modo, descriptografá-la.

Não iremos nos aprofundar neste assunto, porém os mais curiosos podem consultar [5] ou [7] para obter mais informações. Também é possível ver o processo de cripto-análise no conto "O Escaravelho de Ouro" de Edgar Allan Poe (Cameron).

7.3 Tornando seu Código mais Seguro

Devido a facilidade de se descriptografar uma mensagem criptografada com um dos métodos citados neste capítulo, aconselhamos àqueles que queiram saber como tornar um pouco mais difícil o método de cripto-análise consultarem [7] seção 2.5 "*Making a substitution cipher safer*".

Capítulo 8

Resíduos Quadráticos e Lei da Reciprocidade Quadrática

Os Resíduos Quadráticos são importantes para estudarmos métodos de fatoração, mas neste trabalho não iremos estudar estes métodos.

Suponha que p seja um número ímpar, isto é, $p > 2$. Estamos interessados em saber quais dos elementos diferentes de zero $\{1, 2, 3, \ldots, p-1\}$ de $\mathbb{Z}_p$ são quadrados. Se algum $a \in \mathbb{Z}_p^*$ é um quadrado, digamos $a = b^2$, então, a tem precisamente duas raízes quadradas, $\pm b$, pois a equação $x^2 - a = 0$ tem duas soluções em um corpo. Assim, os quadrados em $\mathbb{Z}_p^*$ podem ser determinados pelo cálculo de $b^2 \pmod{p}$ para $b = 1, 2, \ldots, \frac{p-1}{2}$, pois os inteiros restantes até $p-1$ são todos congruentes a $-b$ para cada b, e precisamente metade dos elementos em $\mathbb{Z}_p^*$ são quadrados. Os quadrados em $\mathbb{Z}_p$ são chamados **resíduos quadráticos módulo** p, os outros elementos não-nulos que não são quadrados são chamados de **resíduos não quadráticos módulo** p.

Exemplo 8.1 *Os quadrados em* $\mathbb{Z}_{11}$ *são* $1, 4, 9, 5$ *e* 3*, pois*

$$\begin{aligned} 1^2 &\equiv 1 \,(mod\ 11) \\ 2^2 &\equiv 4 \,(mod\ 11) \\ 3^2 &\equiv 9 \,(mod\ 11) \\ 4^2 &\equiv 5 \,(mod\ 11) \\ 5^2 &\equiv 3 \,(mod\ 11)\,. \end{aligned}$$

Note que

$$\begin{aligned} -1 &\equiv 10 \,(mod\ 11) \\ -2 &\equiv 9 \,(mod\ 11) \\ -3 &\equiv 8 \,(mod\ 11) \\ -4 &\equiv 7 \,(mod\ 11) \\ -5 &\equiv 6 \,(mod\ 11)\,. \end{aligned}$$

Logo, $1, 3, 4, 5$ *e* 9 *são os resíduos quadráticos módulo* 11*, enquanto que* $2, 6, 7, 8$ *e* 10 *são os resíduos não quadráticos módulo* 11*.*

Teorema 8.2 *Seja a um inteiro não divisível por p, p primo maior que 2. Então,*

1. $a^{\frac{(p-1)}{2}} \equiv \pm 1 \, (mod \; p)$.
2. *a é um resíduo quadrático módulo p se, e somente se,*
$$a^{\frac{(p-1)}{2}} \equiv 1 \, (mod \; p) \, .$$
3. *a é um resíduo não quadrático módulo p se, e somente se,*
$$a^{\frac{(p-1)}{2}} \equiv -1 \, (mod \; p) \, .$$

Definição 8.3 (Símbolo de Legendre) *Seja a um inteiro e $p > 2$ um primo. Definimos o símbolo de Legendre $(\frac{a}{p})$ igual a $0, 1$ ou -1, como segue:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{se } p \mid a. \\ 1, & \text{se } a \text{ é um resíduo quadrático módulo } p. \\ -1, & \text{se } a \text{ é um resíduo não quadrático módulo } p. \end{cases}$$

O símbolo de Legendre é uma forma simplificade de verificar se um inteiro a é ou não um resíduo quadrático módulo p.

Teorema 8.4
$$\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \, (mod \; p) \, .$$

Demonstração: Se a é divisível por p, então, ambos os lados são $\equiv 0 \, (\text{mod } p)$. Suponha que $p \nmid a$ e use o Teorema 8.2 e a Definição do Símbolo de Legendre. ■

Teorema 8.5 *O símbolo de Legendre satisfaz as seguintes propriedades:*

1. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
2. *Se $mdc(b, p) = 1$, então $(\frac{b^2}{p}) = 1$.*
3. $(\frac{1}{p}) = 1$ *e* $(\frac{-1}{p}) = (-1)^{\frac{(p-1)}{2}} \, (mod \; p)$.

O ítem 1 do resultado anterior mostra que podemos determinar se um número a é um resíduo quadrático módulo p, isto é, calcular $(\frac{a}{p})$, se sabemos fatorar a e sabemos o símbolo de Legendre de cada fator, ou seja,

$$\left(\frac{a}{p}\right) = \left(\frac{p_1^{\alpha_1}}{p}\right)\left(\frac{p_2^{\alpha_2}}{p}\right) \ldots \left(\frac{p_n^{\alpha_n}}{p}\right), \text{ onde } a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}.$$

O primeiro passo para fazer isto é escrever a como uma potência de 2 vezes um número ímpar, $a = 2^n \cdot b$, onde b é ímpar. Então, queremos saber como calcular $(\frac{2}{p})$.

Teorema 8.6
$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{p}}$$

O próximo resultado irá nos dizer como relacionar $(\frac{p}{q})$ com $(\frac{q}{p})$, onde q e p são primos ímpares.

Teorema 8.7 (Lei da Reciprocidade Quadrática) *Sejam p e q dois primos ímpares. Então,*

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right).$$

Capítulo 9

Logaritmo Discreto e o Problema da Mochila

A partir do Logaritmo Discreto e do Problema da Mochila foram desenvolvidos vários sistemas criptográficos, porém neste trabalho iremos nos ater apenas em exibir estes dois problemas.

9.1 Raízes da Unidade

Em várias situações é útil ter soluções da equação $x^n = 1$ e uma dessas situações é no algoritmo para o cálculo do Logaritmo Discreto, que será visto mais adiante.

Suponha que estamos trabalhando em um corpo finito $\mathbb{Z}_q$. Quantas n-ésimas raízes da unidade existem em $\mathbb{Z}_q$, ou seja, quais são os elementos $x \in \mathbb{Z}_q$ tais que $x^n = 1$?

Proposição 9.1 *Seja g um gerador de $\mathbb{Z}_q^*$. Então:*

1. *g^j é uma raiz n-ésima da unidade se, e somente se, $nj \equiv 0\,(mod\ q-1)$.*
2. *O número de raízes n-ésimas da unidade é $mdc(n, q-1)$.*

Demonstração: *1.* Qualquer elemento de $\mathbb{Z}_q^*$ pode ser escrito como uma potência de g, pois $\langle g \rangle = \mathbb{Z}_q^*$. Assim, uma potência de g é 1 se, e somente se, a potência é divisível por $q-1$, ou seja, $g^k = 1 \Leftrightarrow q-1 \mid k$, pois $\left|\mathbb{Z}_q^*\right| = q-1$. Logo, um elemento g^j é uma raiz n-ésima da unidade, $(g^j)^n = g^{jn} = 1$, se, e somente se, $q-1 \mid jn$, ou seja, $jn \equiv 0\,(\mathrm{mod}\ q-1)$.
2. Seja $d = mdc(n, q-1) \Rightarrow 1 = mdc(\frac{n}{d}, \frac{q-1}{d})$. A equação $nj \equiv 0\,(\mathrm{mod}\ q-1)$ (com j a determinar) é equivalente a

$$\frac{n}{d} j \equiv 0 \left(\mathrm{mod}\ \frac{q-1}{d}\right). \tag{9.1}$$

Como $\frac{n}{d}$ é relativamente primo a $\frac{q-1}{d}$, então, da congruência (9.1) temos que $\frac{q-1}{d} \mid j \Rightarrow j = k\frac{q-1}{d}, k = 0, 1, 2, \ldots$. Em outras palavras, as d potências distintas de $g^{(q-1)/d}$,

$$\left|\left\langle g^{(q-1)/d} \right\rangle\right| = d,$$

são precisamente as n-ésimas raízes da unidade. ■

9.2 Logaritmo Discreto

Suponha que estamos trabalhando em um corpo finito como o $\mathbb{Z}_q$. Se dermos um elemento $y \in \mathbb{Z}_q^*$ que sabemos ser da forma b^x (suponhamos que a base b é "fixa"), como podemos achar a potência de b que é igual a y, isto é, como podemos calcular $x = \log_b y$ (onde "log" tem um significado diferente, mas análogo ao que já conhecemos)? Esta questão é chamada de "problema do logaritmo discreto". A palavra "discreto" distingue a situação do corpo finito da situação clássica (contínua) de um corpo infinito.

Definição 9.2 *Se K é um corpo finito, b um elemento de K e y um elemento de K, o qual é uma potência de b, então, o logaritmo discreto de y na base b é um inteiro x tal que $b^x = y$.*

Exemplo 9.3 *Tomando $K = \mathbb{Z}_{19}$ e seja $b = 2$ e $y = 7$, então o logaritmo discreto de 7 na base 2 é 6, pois $2^6 = 7$, em $\mathbb{Z}_{19}$.*

9.3 Algoritmo para determinar o logaritmo discreto em um corpo finito

Suponhamos que todos os fatores primos de $q-1$ são pequenos. Com esta condição, existe um algoritmo rápido para determinar o logaritmo discreto de um elemento $y \in \mathbb{Z}_q^*$ na base b. Para simplificarmos, devemos supor que b é um gerador de $\mathbb{Z}_q^*$, $\langle b \rangle = \mathbb{Z}_q^*$. Dito isso, descreveremos este algoritmo que é atribuído a Silver, Pohlig e Hellman.

Primeiro, para cada primo p dividindo $q-1$, calculamos as p-ésimas raízes da unidade $r_{p,j} = b^{j(q-1)/p}$ para $j = 0, 1, \ldots, p-1$. Com nossa tabela de $\{r_{p,j}\}$ estaremos prontos para calcular o logaritmo discreto de qualquer $y \in \mathbb{Z}_q^*$. (Note que, se b é fixo, este primeiro cálculo só precisa ser feito uma única vez, depois a mesma tabela é usada para qualquer y.)

Nosso objetivo é achar x, $0 \leq x < q-1$, tal que $b^x = y$. Se

$$q - 1 = \prod_p p^\alpha$$

é a fatoração prima de $q-1$, então é suficiente achar $x \pmod{p^a}$ para cada p dividindo $q-1$; daí, x é unicamente determinado usando o **Teorema Chinês dos Restos**. Assim, fixamos um primo p dividindo $q-1$ e mostraremos como determinar $x \pmod{p^\alpha}$.

Suponha que $x \equiv x_0 + x_1 p + \ldots + x_{\alpha-1} p^{\alpha-1} \pmod{p^\alpha}$ com $0 \leq x_i < p$. Pegando a p-ésima raiz da unidade e sabendo que $y^{(q-1)} = 1$ e $y = b^x$, segue que

$$y^{(q-1)/p} = b^{x(q-1)/p} = b^{\frac{(x_0 + x_1 p + \ldots + x_{\alpha-1} p^{\alpha-1})(q-1)}{p}} = b^{x_0 (q-1)/p} = r_{p,x_0}.$$

Feito isto, comparamos $y^{(q-1)/p}$ com os $\{r_{p,j}\}_{0 \leq j < p}$ e igualamos x_0 com o valor de j com o qual $y^{(q-1)/p} = r_{p,j}$.

A seguir, para calcularmos x_1, substituímos y por

$$y_1 = \frac{y}{b^{x_0}} = \frac{b^x}{b^{x_0}} = \frac{b^{x_0 + x_1 p + \ldots + x_{\alpha-1} p^{\alpha-1}}}{b^{x_0}} = \frac{b^{x_0} b^{x_1 p} \ldots b^{x_{\alpha-1} p^{\alpha-1}}}{b^{x_0}} = (b^{x_1 + x_2 p + \ldots + x_{\alpha-1} p^{\alpha-2}})^p.$$

Então, y_1 tem logaritmo discreto $x - x_0 \equiv x_1 p + \ldots + x_{\alpha-1}p^{\alpha-1} \pmod{p^\alpha}$. Como y_1 é uma p-ésima potência, temos $y_1^{(q-1)/p} = 1$ e

$$y_1^{(q-1)/p^2} = b^{(x-x_0)(q-1)/p^2} = b^{(x_1+x_2p+\ldots+x_{\alpha-1}p^{\alpha-2})(q-1)/p} = b^{x_1(q-1)/p} = r_{p,x_1}.$$

Desta forma, podemos comparar $y_1^{(q-1)/p^2}$ com $\{r_{p,j}\}_{0\leq j<p}$ e igualarmos x_1 com o valor de j para o qual $y_1^{(q-1)/p^2} = \{r_{p,j}\}$.

Deve ser claro de como devemos proceder indutivamente para acharmos tods os $x_0, x_1, \ldots, x_{\alpha-1}$. De fato, para cada $i = 1, 2, \ldots, \alpha - 1$ ajustamos

$$y_i = \frac{y}{b^{x_0+x_1p+\ldots+x_{i-1}p^{i-1}}},$$

o qual tem logaritmo discreto congruente (mod p^α) para $x_ip^i + \ldots + x_{\alpha-1}p^{\alpha-1}$. Como y_i é uma p^i-ésima potência, temos $y_i^{(q-1)/p^i} = 1$ e

$$y_i^{(q-1)/p^{i+1}} = r_{p,x_i}.$$

Assim, igualamos x_i ao valor de j para o qual $y_i^{(q-1)/p^{i+1}} = r_{p,j}$.

Quando tivermos concluído teremos $x \pmod{p^\alpha}$. Depois de fazermos este processo para cada $p \mid q-1$, finalmente utilizaremos o **Teorema Chinês dos Restos** para determinarmos x.

Este algoritmo funciona bem quando todos os primos dividindo $q-1$ são pequenos. É fácil perceber que o cálculo da tabela de $\{r_{p,j}\}$ e a comparação dos $y_i^{(q-1)/p^{i+1}}$ com esta tabela irá tomar muito tempo se $q-1$ é divisível por um primo muito grande.

Exemplo 9.4 *Determinar o logaritmo discreto de* 19 *na base* 5 *em* $\mathbb{Z}_{23}^*$ *usando o algoritmo de Silver-Pohlig-Hellman.*

Solução: Note que $\langle 5 \rangle = \mathbb{Z}_{23}^*$. Neste caso, $q - 1 = 23 - 1 = 22 = 2 \cdot 11$. Primeiro calculamos as p-ésimas raízes da unidade para cada primo p dividindo 22.
Para $p = 2$ temos sempre que

$$\{r_{2,j}\} = \{1, -1\}.$$

Para $p = 11$ temos, utilizando a demonstração da Proposição 9.1, que

$$\{r_{11,j}\} = \left\langle 5^{(23-1)/11} \right\rangle = \left\langle 5^2 \right\rangle = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}.$$

Os elementos dos conjuntos $\{r_{2,j}\}$ e $\{r_{11,j}\}$ estão ordenados.
Agora, seja $19 \equiv 5^x \pmod{23}$. Iremos determinar o x.
Para $p = 2$, devemos encontrar $x \pmod 2$, o qual escrevemos como $x = x_0$.
Calculamos $19^{(23-1)/2} = 19^{11} \equiv 22 \equiv -1 \pmod{23}$ e assim $x = x_0 \equiv 1 \pmod 2$, pois

$$19^{(23-1)/2} = 5^{x_0(23-1)/2} = 5^{x_0 \cdot 11} = r_{2,x_0} = r_{2,1} \equiv -1 \pmod{23}.$$

Para $p = 11$, devemos encontrar $x \pmod{11}$, $x = x_0$. Assim,

$$19^{(23-1)/11} = 19^2 \equiv 16 \pmod{23} \text{ e } 16 = r_{11,4} \Rightarrow x_0 = 4.$$

Logo, $x \equiv 4 \,(\text{mod } 11)$. Resta-nos resolver o sistema

$$\begin{cases} x \equiv 1 \,(\text{mod } 2) \\ x \equiv 4 \,(\text{mod } 11) \end{cases}$$

cuja solução particular $x = 15$ é dada pelo **Teorema Chinês dos Restos**. Portanto, o logaritmo discreto de 19 na base 5 em $\mathbb{Z}_{23}^*$ é 15, ou seja,

$$19 \equiv 5^{15} \,(\text{mod } 23)\,.$$

Exemplo 9.5 *O logaritmo discreto de* 28 *na base* 2 *em* $\mathbb{Z}_{37}^*$ *é* 34*, ou seja,*

$$28 \equiv 2^{34} \,(mod\ 37)\,.$$

Observação 9.6 *A solução completa deste último exemplo é encontrada no livro de Koblitz (1994), página 103.*

9.4 Problema da Mochila

Suponhamos um conjunto com k objetos, os quais seus pesos são conhecidos, e uma mochila, na qual serão colocados alguns dos k objetos. Pesa-se a mochila e pergunta-se: quais objetos estão dentro da mochila?

Mais precisamente, dado um conjunto finito

$$X = \{v_0, v_1, \ldots, v_{k-1}\},$$

os pesos $s_i \in \mathbb{Z}$ associados a cada $v_i \in X$ e um inteiro V, estamos interessados em saber se existe e qual é o subconjunto $Y \subseteq X$ tal que

$$\sum_{v_i \in Y} s_i = V.$$

Ou, equivalentemente, dado o vetor peso

$$\vec{s} = (s_0, s_1, \ldots, s_{k-1}).$$

Pergunta-se: existe um vetor binário

$$\vec{u} = (\epsilon_0, \epsilon_1, \ldots, \epsilon_{k-1}), \epsilon_j \in \{0, 1\},$$

tal que

$$\left\langle \vec{s}, \vec{u} \right\rangle = V \Leftrightarrow \sum_{i=0}^{k-1} \epsilon_i s_i = V?$$

Para efeitos práticos, ao invés do vetor $\vec{u}$ utilizaremos

$$n = (\epsilon_{k-1}\epsilon_{k-2} \ldots \epsilon_1\epsilon_0)_2 = 2^{k-1}\epsilon_{k-1} + 2^{k-2}\epsilon_{k-2} + \ldots + 2\epsilon_1 + \epsilon_0,$$

que é a solução do nosso problema.

Observação 9.7 *Note que o problema pode não ter solução* n*, ou ter várias soluções, ou uma única solução.*

Um caso especial do problema da mochila, que sempre é possível resolver, é o problema onde os pesos são arrajandos na ordem crescente, tendo a seguinte propriedade

$$\sum_{j=0}^{i-1} s_j < s_i, i = 1, 2, \ldots, k-1,$$

ou seja, cada s_i é maior do que a soma dos s_i anteriores. Nesta seção só iremos tratar deste tipo de problema, pois sabemos que é possível resolvê-lo através do seguinte algoritmo (Koblitz).

1. Ajuste W igual a V e tome $j = k$.
2. Começando com ϵ_{j-1} e diminuindo o índice de ϵ, escolha todos os $\epsilon_i = 0$ até chegar ao primeiro i – chamando-o de i_0 – tal que $s_{i_0} \leq W$. Ajuste $\epsilon_{i_0} = 1$.
3. Troque W por $W - s_{i_0}$, ajuste $j = i_0$, e, se $W > 0$ volte ao passo 2.
4. Se $W = 0$, então está terminado. Se $W > 0$ e todos os s_i restantes são maiores do que W, então, sabemos que não esxiste $n = (\epsilon_{k-1}\epsilon_{k-2}\ldots\epsilon_1\epsilon_0)_2$ solução do problema.

A solução (se existe) é única.

Exemplo 9.8 *Resolver o problema da mochila para os cinco objetos com vetor peso associado a eles dado por* $\vec{s} = (2, 3, 7, 15, 31)$ *e a mochila com peso total* $V = 23$.

Solução: Sabemos que $s_0 = 2, s_1 = 3, s_2 = 7, s_3 = 15$ e $s_4 = 31$. Como $V = 23 < 31 \Rightarrow s_4 = 31$ não está na mochila $\Rightarrow \epsilon_4 = 0$. Sendo $s_3 = 15 < V = 23 \Rightarrow s_3$ está na mochila, logo, $\epsilon_3 = 1$. Tomando

$$V_1 = V - s_3 = 23 - 15 = 8,$$

temos que $s_2 = 7 < V_1 = 8 \Rightarrow s_2$ está na mochila. Assim,

$$V_2 = V_1 - s_2 = 1.$$

Desta forma, s_1 e s_0 não podem estar na mochila $\Rightarrow \epsilon_1 = \epsilon_0 = 0$ e $V_2 = 1 > 0$. Portanto, para $V = 23$ e $\vec{s} = (2, 3, 7, 15, 31)$ não existe $n = (\epsilon_4\epsilon_3\epsilon_2\epsilon_1\epsilon_0)_2$ satisfazendo $\sum_{i=0}^{k-1} \epsilon_i s_i = V$.

Quando mencionamos que s_i (não) está na mochila, queremos dizer que o objeto v_i (não) está na mochila.

Exemplo 9.9 *Resolver o problema da mochila para os sete objetos com vetor peso associado a eles dado por* $\vec{s} = (1, 3, 5, 11, 23, 44, 89)$ *e a mochila com peso total* $V = 139$.

Solução: Como $s_6 = 89 < V \Rightarrow \epsilon_6 = 1$. Assim, $V_1 = V - s_6 = 50$. Logo, $s_5 = 44 < V_1 \Rightarrow \epsilon_5 = 1$ e $V_2 = V_1 - s_5 = 6$. Como $s_4 = 23$ e $s_3 = 11$ são maiores que $V_2 \Rightarrow \epsilon_4 = \epsilon_3 = 0$, mas $s_2 = 5 < V_2 \Rightarrow \epsilon_2 = 1$ e $V_3 = V_2 - s_2 = 1$. Logo,

$s_1 = 3 > V_3 \Rightarrow \epsilon_1 = 0$ e $s_0 = 1 \leq V_3 \Rightarrow \epsilon_0 = 1$. Assim, $V_4 = 0 \Rightarrow$ este problema tem uma única solução

$$n = (1100101)_2 = 101.$$

Note que,

$$\sum_{i=0}^{6} \epsilon_i s_i = 1{\cdot}1+0{\cdot}3+1{\cdot}5+0{\cdot}11+0{\cdot}23+1{\cdot}44+1{\cdot}89 = 1+5+44+89 = 139 = \left\langle \vec{s}, \vec{u} \right\rangle,$$

onde $\vec{u}= (1, 0, 1, 0, 0, 1, 1)$. Podemos concluir que v_6, v_5, v_2 e v_0 são os únicos objetos que estão na mochila de peso total $V = 139$.

Capítulo 10

Criptografia RSA

10.1 Conceitos Básicos

O sistema de criptografia visto no Capítulo 7 é chamado simétrico, porque, como foi visto, a chave usada para codificação é, de certa forma, igual à chave usada para decodificação, ou, equivalentemente, a partir de uma delas obtemos a outra utilizando o Algoritmo Euclidiano. Por isso, os sistemas simétricos são interessantes quando um transmissor conversa apenas com um receptor. Caso um transmissor converse com vários receptores, então todos os receptores estarão aptos para decodificar o texto-cifrado. Para contornar este problema, neste capítulo apresentaremos um outro sistema de criptografia, chamado RSA, que foi desenvolvido por Rivest, Shamir e Adleman em 1978.

O RSA é um sistema criptográfico assimétrico e este tipo de sistema diferencia-se dos simétricos justamente pelo fato de permitir que vários indivíduos conversem entre si, onde cada um terá uma chave de codificação que é pública, ou seja, todos a conhecem, e por isto este tipo de sistema também é conhecido por sistema de criptografia com chave pública, e uma outra chave de decodificação que é mantida secreta.

No sistema assimétrico é, de um modo geral, impossível determinar uma chave a partir da outra, isto é, se sei a chave de codificação, já que esta é pública, é muito difícil obter a chave de decodificação.

10.2 Mecânica do Sistema Assimétrico

Suponhamos que exista um grupo de usuários u_j, $j = 1, 2, \ldots, n$ e eles desejam se comunicar entre si. Primeiro os usuários devem determinar o alfabeto que irão utilizar e a associação de cada símbolo do alfabeto com um número inteiro, do mesmo modo que foi feito no Exemplo 7.2. Então, cada usuário u_j irá determinar um par de chaves $k_{c,j}$ e $k_{d,j}$ tais que

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

onde $\mathbf{u}$ é uma mensagem unitária do texto-original. A chave $k_{d,j}$ é mantida secreta e irá servir para o usuário u_j decodificar as mensagens criptografadas com a chave pública de codificação $k_{c,j}$.

Feito isso, se um usuário u_i deseja enviar uma mensagem $\mathbf{u}$ ao usuáro u_j, então, u_i utiliza a chave pública de codificação $k_{c,j}$ na mensagem $\mathbf{u}$ e obtem a mensagem codificada $\mathbf{d}$,

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

Em seguida o usuário u_i envia a mensagem codificada $\mathbf{d}$ a u_j e este ao recebê-la, decofica aplicando a chave secreta de decofição $k_{d,j}$, recuperando, assim, a mensagem original $\mathbf{u}$,

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

Note que, caso um outro usuário u_k interceptasse a mensagem $\mathbf{d}$, enviada de u_i para u_j, ele não teria como decodificá-la, pois não possui a chave secreta de decodificação $k_{d,j}$.

10.3 O Sistema RSA

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 para determinar $n_i = p_i \cdot q_i$ e aleatoriamente um inteiro qualquer t_i tal que

$$mdc(t_i, \phi(n_i)) = 1.$$

A seguir u_i calcula $r_i \equiv t_i^{-1} \pmod{\phi(n_i)}$. 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

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

e, pelo Corolário 6.6, o processo de decodificação é dado pela função

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

Seja $\mathbb{F}$ 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

$$x = x_{k-1}n^{k-1} + \ldots + x_2n^2 + x_1n + x_0 \in \mathbb{Z}_{n^k}, x_r \in \{0, 1, \ldots, k-1\},$$

e cada um destes blocos será codificado em um só bloco com l símbolos, com $k < l$. Para fazer isto, cada usuário u_i deve escolher os dois números primos distintos p_i e q_i de modo que $n_i = p_iq_i$ 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 10.1 *A correspondência biunívoca entre o alfabeto $\mathbb{F}$ e os números inteiros é a mesma dada no Exemplo 7.2 e escolhemos $k = 3$ e $l = 4$. Para enviarmos a mensagem*

$$\text{“FIM”}$$

para um usuário u_j com chave de codificação

$$k_{c,j} = (35183, 4459),$$

primeiro determinamos a equivalência numérica

$$\begin{array}{c} FIM \\ \updownarrow \\ 5 \cdot 26^2 + 8 \cdot 26 + 12 = 3600 \end{array}$$

e, então, calculamos

$$3600^{4459} \, (mod \; 35183) \, ,$$

que é

$$8808 = 0 \cdot 26^3 + 13 \cdot 26^2 + 0 \cdot 26 + 20$$

e equivale a mensagem “ANAU”. O usuário u_j sabe a chave de decodificação

$$k_{d,j} = (35183, 9139)$$

e, então, calcula

$$8808^{9139} \, (mod \; 35183) \, ,$$

que equivale a $3600 = 5 \cdot 26^2 + 8 \cdot 26 + 12$ e, portanto, recupera a mensagem “FIM”.

Observação 10.2 *O usuário u_j gerou suas chaves multiplicando os números primos $p_j = 151$ e $q_j = 233$ para obter n_j, depois escolheu aleatoriamente o número t_j tal que $mdc(t_j, \phi(n_j)) = 1$. Finalmente, determinou $r_j \equiv t_j^{-1} \, (mod \; \phi(n_j))$. Note que os números p_j, q_j e r_j permanecem secretos.*

A segurança do sistema RSA está na dificuldade em fatorar o inteiro n_i. Caso n_i fosse fatorado, poderiamos determinar o inteiro r_i e, consequentemente, a chave de decodificação $k_{d,i} = (n_i, r_i)$.

10.4 Assinatura

Uma maneira de enviar assinaturas pelo sistema RSA é a seguinte: o usuário u_i de posse da sua chave de decodificação $k_{d,i}$ a utiliza na sua assinatura $\mathbf{a}$

$$k_{d,i}(\mathbf{a}) = \mathbf{c}_i.$$

Em seguida, utiliza a chave de codificação do usuário, digamos u_j, com o qual deseja se comunicar e aplica esta chave na assinatura “codificada” $\mathbf{c}_i$,

$$k_{c,j}(\mathbf{c}_i) = \mathbf{c}_{ij}.$$

Feito isso, o usuário u_i envia ao usuário u_j a assinatura $\mathbf{c}_{ij}$ e este ao recebê-la aplica sua chave de decodificação $k_{d,j}$ obtendo $\mathbf{c}_i$,

$$k_{d,j}(\mathbf{c}_{ij}) = \mathbf{c}_i.$$

Ao perceber que o texto ainda está criptografado e sabendo que foi enviado por u_i, então u_j aplica a chave de codificação $k_{c,i}$ no texto $\mathbf{c}_i$ obtendo, assim, a assinatura no texto-original $\mathbf{a}$,

$$k_{c,i}(\mathbf{c}_i) = \mathbf{a}.$$

Capítulo 11

Conclusão

Podemos observar, depois deste ano de estudos, que a Teoria dos Números, principalmente a Aritmética Modular, é fundamental para quem deseja iniciar seus estudos na arte de codificar mensagens, a Criptografia.

Também foi possível desenvolver um programa em linguagem de programação PHP, que criptografa e descriptografa mensagens, utilizando o conteúdo visto no Capítulo 7. Este programa nos auxiliou para fazermos o Exemplo 7.2 e com a construção deste programa notamos que a Criptografia é um processo algorítmico facilmente aplicado a linguagens de programação computacionais. O processo de elaboração deste programa é encontrado no site

http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=2144

e o programa está a disposição no endereço

http://www.mat.ufpb.br/~camat/criptografa_ver03.php.

Tivemos conhecimento de alguns sistemas critptográficos ao analisarmos o Logaritmo Discreto e o Problema da Mochila e pudemos concluir que o sistema criptográfico RSA ainda é o mais seguro na transmissão de mensagens, pois não existe um algoritmo que fatore rapidamente um número inteiro qualquer (desvendando, desta forma, sua chave de decodificação).

Por outro lado, ao constatarmos que na criptografia critérios de primalidade são de grande importância, pretendemos no futuro estudar o algoritmo AKS, que informa se um determinado número é primo ou não. Além disso, aspiramos nos aprofundar ainda mais no estudo dos métodos criptográficos fundamentados no Problema da Mochila e no Logaritmo Discreto, que, como foi dito acima, tivemos conhecimento no decorrer deste trabalho. Por fim, vale ressaltar, que é de nosso interesse estudar o tempo estimado que se gasta ao fazer determinado cálculo matemático, no intuito de se encontrar o caminho mais eficaz para fazê-lo.

Referências Bibliográficas

[1] Silva, A. A. *Números, Relações e Criptografia*. Departamento de Matemática - UFPB.

[2] Sidki, S. *Introdução à Teoria dos Números*. 10.º Colóquio Brasileiro de Matemática, IMPA, 1975.

[3] Lima, E. L. *Curso de Análise*, vol. 1. Projeto Euclides, IMPA, 2002.

[4] Eric W. Weisstein. "Finite Field." From MathWorld – A Wolfram Web Resource. *http://mathworld.wolfram.com/FiniteField.html*.

[5] Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed., Springer, 1994.

[6] Koblitz, *Algebraic Aspects of Cryptography*, Volume 3. Springer, 1999.

[7] Cameron, P. J. *Notes on Cryptography*. *http://www.maths.qmw.ac.uk/%7Epjc/notes/crypt.pdf*

[8] Poe, E. A. *Histórias Extraordinárias*, Abril Cultural, 1978. (p. 333 a 375)