UNIVERSIDADE FEDERAL DA PARAÍBA
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática em Rede Nacional

UFPB

PROFMAT

A Matemática Via Algoritmo de Criptografia ElGamal [†]

por

Glauber Dantas Morais

sob orientação do

Prof. Dr. Bruno Henrique Carvalho Ribeiro

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2013
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

A Matemática Via Algoritmo de Criptografia ElGamal

por

Glauber Dantas Morais

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática.

Aprovada por:

Prof. Dr. Bruno Henrique Carvalho Ribeiro -UFPB (Orientador)

Prof. Dr. Antônio de Andrade e Silva - UFPB

Prof. Dr. Jamilson Ramos Campos - UFPB

Agosto/2013

Agradecimentos

Agradeço primeiramente a Deus, pois sem ele nada seria possível. Aos meus pais João de Deus Morais e Maria Isabel Dantas Morais que me ensinaram que a educação é a melhor herança deixada por eles. Aos meus irmãos Yuri Dantas Morais e Aldrin José Dantas Morais e suas respectivas esposas Suzy Karine e Danielle Barbosa, que me ajudaram e apoiaram durante todo o percurso.

A todos os professores e colegas que tive na vida que compartilharam comigo seus conhecimentos e suas experiências, principalmente aqueles que fazem parte do PROFMAT no polo de João Pessoa.

Ao professor João Marcos do Ó e a professora Flávia Jerônimo pelos seus esforços para fazer do PROFMAT uma realidade na UFPB.

Ao professor Bruno Ribeiro que me ajudou ao longo de todo o curso, principalmente nessa dissertação, sanando as eventuais dúvidas que surgiram e sugerindo textos para enriquecer o trabalho.

Agradeço Principalmente a minha esposa Valdeni Nunes de Andrade, que me acompanhou durante o mestrado com paciência e me incentivou a sempre buscar o melhor de cada situação, visando a busca de conhecimentos e diversão nesses momentos.

Dedicatória

A minha esposa Valdeni Nunes de Andrade, que me acompanhou nesse momento de alegria e sucesso, a minha família, em particular aos meus pais João de Deus Morais e Maria Izabel Dantas Morais, que me educaram para a vida.

Resumo

O algoritmo de criptografia escrito pelo egípcio Taher ElGamal calcula logaritmos discretos com elementos de um Grupo Cíclico finito G. Esses elementos possuem propriedades que estudaremos no decorrer do capítulo 1. Conhecendo as definições e algumas propriedades estudadas, poderemos definir e calcular logaritmos discretos, utilizando conhecimentos da Aritmética dos Restos e Congruências, bem como o Teorema Chinês dos Restos. Vamos estudar algoritmos de chave pública, em particular o algoritmo escrito por ElGamal, buscando entender as dificuldades apresentadas por ele e mostrar suas aplicações no campo da Criptografia. Apresentaremos uma sequencia de atividades, voltadas para estudantes do primeiro ano do Ensino Médio, visando o aprendizado de alguns assuntos abordados no trabalho.

Palavras chave: ElGamal, grupos cíclicos, raiz primitiva, logaritmo discreto, algoritmo de criptografia, chave pública.

Abstract

The encryption algorithm written by Egyptian Taher ElGamal computes discrete logarithms with elements of a finite group G Cyclical. These elements have properties that during the study Chapter 1. Knowing the definitions and some properties studied, we can define and compute discrete logarithms, using knowledge of arithmetic and congruence of Remains and Theorem Remainder of Chinese. We will study public key algorithms, in particular the algorithm written by ElGamal, seeking to understand the difficulties presented by it and show its applications in the field of cryptography. We present a sequence of activities, aimed at students of the first grade of high school, targeting the learning of some subjects covered at work.

Keywords: ElGamal, cyclic groups, primitive root, discrete logarithm, encryption algorithm, public key.

Sumário

Lista de Figuras

Introdução

Este trabalho tem por finalidade explicar a matemática por trás do algoritmo de Criptografia ElGamal. Através dele, professores de matemática do nível Fundamental e Médio podem explicar como acontece a troca de mensagens sigilosas pela internet, assunto que gera interesse em pessoas que gostam de aprender a linguagem computacional. Dessa forma o professor pode incentivar seus alunos na aprendizagem da "Matemática Abstrata", podendo inclusive fazer com que esse aluno ingresse num curso de matemática no nível Superior.

A principal dificuldade nesse algoritmo é o cálculo de logaritmos discretos que, diferente do logaritmo de um número real, podem não possuir solução. Para entendermos essa dificuldade, começamos mostrando a Teoria dos Grupos no primeiro capítulo, em particular explicamos como encontrar os elementos do grupo cíclico $\mathbb{Z}_p^*$, com p primo. Destacamos o "Pequeno Teorema de Fermat" e o "Teorema Chinês dos Restos" como ferramentas fundamentais para a realização dos cálculos no decorrer do trabalho.

No capítulo 2 apresentamos as definições e propriedades dos logaritmos discretos, mostrando como calcular o logaritmo discreto de um elemento b do grupo $\mathbb{Z}_p^*$ na base a, com $a, b \in \mathbb{Z}_p^*$, e apresentamos um algoritmo que serve para calcular esse logaritmo quando o número primo p for muito grande, o "Algoritmo de Silver, Pohlig e Hellman". Porém, mesmo com o auxílio desse logaritmo, o leitor pode perceber que os cálculos são complexos e demorados, esse fato é conhecido como "Problema do logaritmo discreto" e é a base para o algoritmo de criptografia ElGamal.

No capítulo 3, realizamos uma introdução histórica sobre algoritmo e criptografia, mostrando exemplos no cotidiano escolar de um aluno no nível Fundamental e Médio. Depois explicamos o que é e como funciona os sistemas de criptografia de "chave pública", também conhecidos como "criptossistemas", e mostramos dois exemplos desses sistemas, o mais antigo e o mais utilizado na troca de informações sigilosas.

O capítulo 4 é dedicado ao algoritmo de criptografia de ElGamal. Nele mostramos como acontece a troca de mensagens e explicamos a matemática que é utilizada tendo como base os capítulos anteriores. Mostramos também as duas formas que um invasor poderia tentar quebrar o algoritmo, recuperando a chave particular ou forjando assinaturas sem recuperar a chave particular. Mostramos que são poucas

as chances desse invasor obter sucesso sem saber da chave particular.

No capítulo 5, apresentamos uma sequência de 3 atividades sobre alguns assuntos abordados no trabalho que um professor de matemática pode aplicar numa sala de aula da 1º ano do Ensino Médio, visando mostrar como utilizar o algoritmo de criptografia ElGamal para trocar mensagens criptografadas e estimular a curiosidade dos alunos sobre os assuntos abordados no trabalho. O leitor interessado pode utilizar essas atividade para criar outras com a mesma finalidade, como "resolver um sistema de congruências utilizando o Teorema Chinês dos Restos" ou "calcular logaritmos discretos com o auxílio do Algoritmo de Silver, Pohlig e Hellman".

Capítulo 1

Grupos, Subgrupos e o Grupo $\mathbb{Z}_p$

Estudaremos algumas propriedades dos grupos, subgrupos e o grupo cíclico $\mathbb{Z}_p$, com p primo. Esse estudo será estritamente necessário para calcularmos os logaritmos discretos, bem como o estudo do algoritmo de criptografia ElGamal, pois o mesmo é definido com elementos de um grupo cíclico finito, por isso precisamos saber "o que significa um grupo ser cíclico e finito?" Para responder essa pergunta vamos primeiro definir "grupo" e em seguida vamos ver algumas de suas propriedades.

1.1 Grupo

1.1.1 Grupo

O estudo dos Grupos é realizado no Ensino Superior em disciplinas iniciais de Álgebra, esse estudo é importante, pois nele é apresentado um conjunto e uma operação que deve satisfazer certas propriedades para obtermos um grupo. Em [3] "Grupo" é definido da seguinte forma:

Definição 1 *Um conjunto G com uma operação*

$$G \times G \longrightarrow G$$

$$(a, b) \longmapsto a \cdot b$$

é um grupo se as seguintes condições são satisfeitas:

1. *A operação é associativa, isto é,*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad \forall a, b, c \in G.$$

2. *Existe um elemento neutro, isto é,*

$$\exists\ e \in G \text{ tal que } a \cdot e = e \cdot a = a.$$

3. *Todo elemento possui um elemento inverso, isto é,*

$$\forall\ a \in G,\ \exists\ b \in G \text{ tal que } a \cdot b = \cdot a = e.$$

Denotamos b por a^{-1}

Note que na definição de grupo, é preciso que o conjunto e a operação tenham "elemento neutro" e todos os elementos devem possuir "elemento inverso". É comum então aparecer as seguintes perguntas: "Será que existe mais de um elemento neutro em um grupo?" ou "algum elemento pode possuir mais de um inverso?" Os teoremas a seguir respondem essas perguntas.

Teorema 2 *O elemento neutro de um grupo é único.*

Demonstração: Suponha que existem $e, e' \in G$ tais que os dois sejam elementos neutros de G. Como e é elemento neutro de G temos que:

$$e = e \cdot e'$$

e e' é elemento neutro de G, temos que:

$$e' = e' \cdot e$$

$$\therefore e' = e$$

Portanto o elemento neutro de um grupo é único. ■

Teorema 3 *O elemento inverso de qualquer elemento de um grupo é único.*

Demonstração: Suponha que existem $b, c \in G$ dois elementos inversos de $a \in G$. Da definição de grupo temos:

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

Portanto o elemento inverso de qualquer elemento de um grupo é único. ■

Dizemos que um grupo é *abeliano* ou *comutativo* se ele também apresentar a propriedade comutativa, isto é,

$$a \cdot b = b \cdot a, \ \forall a, b \in G$$

Esse tipo de grupo é importante para nossos estudos, pois veremos ainda nesse capítulo que todo grupo cíclico é abeliano.

1.1.2 Subgrupos

No estudo dos grupos é essencial sabermos o que é um subgrupo, principalmente pelo fato de que um grupo cíclico é um subgrupo do grupo principal estudado, ou seja, o grupo $\mathbb{Z}_p^*$ é um subgrupo de $\mathbb{Z}$. Subgrupo é definido em [3] da seguinte forma:

Definição 4 *Seja $(G, \cdot)$ um grupo. Um Subconjunto não-vazio H de G é um subgrupo de G (denotamos $H < G$) quando, com a operação de G, o conjunto H é um grupo, isto é, quando as seguintes condições são satisfeitas:*

1. $h_1 \cdot h_2 \in H, \forall\ h_1, h_2 \in H$;
2. $h_1 \cdot (h_2 \cdot h_3) = (h_1 \cdot h_2) \cdot h_3, \forall\ h_1, h_2, h_3 \in H$
3. $\exists\ e \in H$ *tal que* $e \cdot h = h \cdot e = h, \forall\ h \in H$
4. *para cada* $h \in H\ \exists\ h^{-1} \in H$ *tal que* $h \cdot h^{-1} = h^{-1} \cdot h = e$

Note que as condições 2, 3, 4 decorrem do fato de H ser um grupo, já a primeira condição diz que a operação $(\cdot)$ está bem definida em H.

A proposição a seguir estabelece quando um subconjunto H é um subgrupo de G, sem precisar verificar se as condições da Definição 4 são satisfeitas.

Proposição 1 *Seja H um subconjunto não vazio do grupo G. H é um subgrupo de G se, e somente se, as seguintes condições são satisfeitas:*

1. $h_1 \cdot h_2 \in H, \forall\ h_1, h_2 \in H$

2. $h^{-1} \in H, \forall\ h \in H$

Demonstração: Seja $H < G$, temos que a operação está bem definida em H (definição de subgrupos), da mesma forma, cada elemento tem um inverso no próprio subgrupo, pois todo subgrupo é um grupo.

Vamos provar agora que se apenas as duas condições são satisfeitas, H é um subgrupo, ou seja, vamos verificar as quatro condições dos subgrupos. A primeira condição é a mesma nos dois casos, portanto ela é satisfeita. A segunda condição é satisfeita pois a operação do subgrupo é associativa para todos elementos de H.

Seja $h \in H$ por 2 temos que $h^{-1} \in H$, por 1 temos que $h \cdot h^{-1} \in H$, como $h \cdot h^{-1} = e$, temos que $e \in H$, ou seja, o elemento neutro pertence a H, portanto, a terceira condição é satisfeita e a quarta condição também. ■

Vamos agora começar a "construir" o grupo $\mathbb{Z}_p^*$, ou seja, vamos mostrar como são os elementos desse conjunto e a operação que será utilizada. Primeiro vamos definir uma operação para esse conjunto que satisfaça as condições de subgrupo.

Definição 5 *Sejam $(G, \cdot)$ um grupo e $a \in G$. Definimos as potências de a da seguinte forma:*

$$\begin{aligned} a^0 &= e; \\ a^n &= a^{n-1} \cdot a, \quad com\ n \in \mathbb{N}; \\ a^{-n} &= (a^n)^{-1}, \quad com\ n \in \mathbb{N}. \end{aligned}$$

Denotamos por $\langle a \rangle$ o conjunto de todas as potências de a, ou seja:

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

Vamos mostrar a seguir que essa Definição faz com que $\langle a \rangle$ seja subgrupo G, dessa forma poderemos caracterizar o Grupo $\mathbb{Z}_p^*$.

Afirmação 1 *$\langle a \rangle$ é um subgrupo de G.*

Demonstração: Vamos verificar se as duas condições da Proposição 1 são satisfeitas:

1. Sejam $n, m \in \mathbb{Z}$, temos que $a^n, a^m \in \langle a \rangle$, com isso $a^n \cdot a^m = a^{n+m}$. Como $n + m \in \mathbb{Z} \Rightarrow a^{n+m} \in \langle a \rangle$;

2. Por definição, $a^{-1} \in \langle a \rangle$.

Portanto, $\langle a \rangle$ é subgrupo de G. ■

Note que no conjunto das potências podemos construir um subgrupo utilizando as potências de um elemento, com isso poderemos caracterizar esse elemento como o "gerador" do subgrupo.

Definição 6 *$\langle a \rangle$ é o* **subgrupo gerado** *por a. Chamamos a de* **gerador** *de $\langle a \rangle$*

Podemos agora denominar grupos que podem ser gerados por um elemento, com isso voltaremos nossos estudos para esse tipo de grupo.

Definição 7 *Um grupo G é* **cíclico** *quando ele pode ser gerado por um elemento de G.*

Agora que sabemos o que é um grupo cíclico, podemos procurar saber o "tamanho" desse grupo, ou seja, da mesma forma que um conjunto possui uma cardinalidade, um grupo pode possuir um "tamanho", basta verificar o número de elementos desse grupo.

Definição 8 *A* **ordem** *de um grupo G é o número de elementos em G. Ela será denotada por $|G|$.*

Note que um grupo pode ter uma ordem "finita", quando o número de elementos desse grupo é finito, ou uma ordem infinita, quando o número de elementos desse grupo é infinito.

Como um grupo cíclico é um grupo que é gerado por um elemento, podemos definir a ordem de um elemento do Grupo G da seguinte forma:

Definição 9 *Chama-se ordem de um elemento $a \in G$ ao menor inteiro positivo n tal que $a^n = e$. Usamos a notação $O(a)$ para indicarmos a ordem de um elemento.*

A Ordem de um elemento de um grupo cíclico possui as seguintes propriedades:

1. $O(e) = 1$

   Demonstração: Trivial ■

2. $O(a) = O(a^{-1})$

   Demonstração: Temos pela Definição 9 que $O(a) = n \Rightarrow a^n = e$, pela Definição 5 $a^{-n} = (a^n)^{-1} = e$. Seja $k \in \{1, 2, \ldots, n-1\}$ pela Definição 9 sabemos que $a^k \neq e$, agora suponha que $(a^{-1})^k = e$, então existe $j \in \{1, 2, \ldots, n-1\}$ tal que $(a^j)^{-1} = e$, assim, pela unicidade do inverso, existe $j \in \{1, \cdots, n-1\}$ tal que $a^j = e$ o que é absurdo. ■

3. Se $a = cbc^{-1}$ então $O(a) = O(b)$

   Demonstração: Suponha que $O(a) = n$, vamos provar que $O(b) = n$. Temos que

   $$a^n = (cbc^{-1})^n = (cbc^{-1}) \cdots (cbc^{-1}) = cb^n c^{-1}$$

   Assim, de

   $$cb^n c^{-1} = a^n = e$$

   segue que

   $$b^n = e$$

   Suponha agora que existe $j \in \{1, \ldots, n-1\}$ tal que $b^j = e$: De $a = cbc^{-1}$ resulta $b = c^{-1}ac$ donde $b^j = c^{-1}a^j c = e$. Assim, existe $j \in \{1, \ldots, n-1\}$ tal que $a^j = e$ o que é absurdo já que $O(a) = n$. ■

4. $O(a^m) \leq O(a); \forall m \in \mathbb{Z}$.

   Demonstração: Suponha que $O(a) = n$ e que $O(a^m) = k$: Ora, pela Definição 9, k é o menor inteiro positivo tal que $(a^m)^k = e$: Mas $(a^m)^n = e$; então $n \geq k$. ■

5. Seja $O(a) = n$. Se $\text{mdc}(m; n) = 1$ então $O(a^m) = O(a) = n$.

   Demonstração: Por 4, temos que $O(a^m) \leq n$, vamos provar que $O(a) = n \leq O(a^m)$. Como $\text{mdc}(m; n) = 1$, temos que existem inteiros x, y tais que

   $$1 = xm + yn$$

   Então, $a = a^{xm+yn} = (a^m)^x (a^n)^y = (a^m)^x$. Assim, de $a = (a^m)^x$, concluímos que $O(a) \leq O(a^m)$. ■

Proposição 2 *Se $O(a) = n$ e $m \in \mathbb{Z}$, então $a^m = e$ se, e somente se, $m = kn; k \in \mathbb{Z}$, ou seja m é múltiplo de n:*

Demonstração: (Condição Necessária) Suponha que $O(a) = n$ e $a^m = e$; onde $m \in Z$, vamos provar que m é múltiplo de n. Suponha que $m \in \mathbb{Z}_+$. Então, pela Definição 9, $m \geq n$. Temos que

$$m = nq + r; r \in \{0, \ldots, n-1\}; q, r \in \mathbb{Z}_+.$$

Então

$$e = a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = a^r.$$

Assim, $r = 0$ pois $r \in \{0, \ldots, n-1\}$ e $O(a) = n$. Portanto

$$a^m = a^{nq}a^r = a^{nq}e = a^{nq}$$

.

(Condição Suficiente) Suponha que $m = nk; k \in \mathbb{Z}$. Então $a^m = a^{nk} = (a^n)^k = e$. ■

O próximo teorema vai relacionar a ordem de um elemento com o tamanho do grupo cíclico. Como corolário desse teorema, poderemos saber se um elemento é gerador através da ordem desse elemento.

Teorema 10 *Seja $a \in G$. Se $O(a) = n$, então $\langle a \rangle$ é um subgrupo cíclico G com n elementos.*

Demonstração: Dado $a \in G$. Pela Definição 9 temos

$$O(a) = n \Rightarrow a^n = e$$

Agora calculando as potências de a, pela Definição 5, obtemos

$$a^{n+1} = a^n \cdot a = e \cdot a = a$$
$$a^{n+2} = a^{n+1} \cdot a = a \cdot a = a^2$$
$$a^{n+3} = a^{n+2} \cdot a = a^2 \cdot a = a^3$$
$$\vdots$$
$$a^{n+n-1} = a^n \cdot a^{n-1} = e \cdot a^{n-1} = a^{n-1}$$
$$a^{n+n} = a^{n-1} \cdot a = a^n = e$$

Com isso, temos que os elementos de $\langle a \rangle$ são obtidos de forma cíclica e $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. Portanto, $\langle a \rangle$ é um subgrupo cíclico com n elementos ■

O Corolário a seguir é consequência imediata do Teorema 10.

Corolário 2.1 *$| G | = n$ e $O(a) = n$ se, e somente se, $\langle a \rangle = G$.*

O corolário acima nos garante que a é um gerador de G quando o subgrupo gerado por a possui a mesma quantidade de elementos do grupo G. Esse fato será de fundamental importância na próxima seção, pois é com seu uso que poderemos saber quando um elemento de $\mathbb{Z}_p^*$ pode ser gerado por algum de seus elementos.

Com essa breve introdução da teoria dos grupos, podemos começar a estudar o grupo cíclico $\mathbb{Z}_p^*$. As definições e teoremas apresentados servirão para "construir" esse grupo.

1.2 O grupo $\mathbb{Z}_p$

Estudaremos agora a teoria dos grupos cíclicos finitos $\mathbb{Z}_p$ com p primo. Esse estudo é importante para podermos trabalhar com os logaritmos discretos, objetivo principal do segundo capítulo desse texto. Para isso vamos definir a seguinte relação entre números inteiros:

Definição 11 *Seja n um número inteiro diferente de zero. Diremos que dois números inteiros a e b são* **congruentes** *módulo n quando os restos de sua divisão euclidiana por n são iguais. Quando os números a e b são congruentes módulo n, escrevemos da seguinte forma:*

$$a \equiv b(mod\ n)$$

Observação 1 *Note que a relação de congruência é uma relação de equivalência, pois:*

1. $a \equiv a(mod\ n)$*(reflexiva);*
2. $a \equiv b(mod\ n) \Rightarrow b \equiv a(mod\ n)$*(simétrica);*
3. $a \equiv b(mod\ n)\ e\ b \equiv c(mod\ n) \Rightarrow a \equiv c(mod\ n)$*(transitiva).*

Como os possíveis restos da divisão euclidiana de um número a por n é um número menor do que n, é fácil ver que esse número é congruente a um, e somente um, dos números $0, 1, \ldots, n-1$.

É possível saber se dois números inteiros são congruentes sem precisar realizar a divisão euclidiana desses números por n, isso facilitará os estudos e algumas demonstrações, pois podemos trabalhar com critérios de divisibilidade dos números inteiros.

Proposição 3 *Sejam $a, b \in \mathbb{Z}_+$ e $b \geq a$. Temos que:*

$$a \equiv b(mod\ n) \Leftrightarrow n \mid b - a$$

Demonstração: Dados $a, b \in \mathbb{Z}_+$, pela Definição 11, temos que

$$a \equiv b(mod\ n) \Leftrightarrow a = nq + r\ e\ b = np + r.$$

Com isso,

$$b-a = np+r-(nq+r) \Leftrightarrow b-a = np-nq+r-r \Leftrightarrow b-a = n(p-q).$$

Como p e q são números inteiros, $p-q$ também é um número inteiro, ou seja $n \mid b-a$, portanto, $a \equiv b(mod\ n) \Leftrightarrow n \mid b-a$ ■

Vimos anteriormente que a congruência é uma relação de equivalência. Veremos a seguir mais algumas consequências dessa relação que servirão para os estudos dos logaritmos discretos.

Teorema 12 *Sejam $a, b, c, d, x \in \mathbb{Z}$ e $n \in \mathbb{N}$. As seguintes condições são satisfeitas:*

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

2. *Se $a \equiv b(mod\ n)$, então $ax \equiv bx(mod\ n)$;*

3. *Se $a \equiv b(mod\ n)$, então $a^k \equiv b^k(mod\ n), \forall k \in \mathbb{N}$.*

Demonstração:

1 Pela Proposição 3, temos que $n \mid b-a$ e $n \mid c-d$, ou seja, existem $k, q \in \mathbb{N}$ tais que $nk = b-a$ e $nq = c-d$. Daí,

$$(b+d)-(a+c) = (b-a)+(d-c) = nk+nq = n(k+q) \Leftrightarrow a+c \equiv b+d(mod\ n).$$

De maneira análoga temos,

$$ac-bd = (b+kn)(d+qn)-bd = bd+bqn+dkn+kqn^2-bd = n(bq+dk+kqn) \Leftrightarrow$$

$$\Leftrightarrow ac \equiv bd(mod\ n);$$

2 Pela Proposição 3, temos que $n \mid b-a$. Logo,

$$bx-ax = x(b-a) = xnq \Leftrightarrow ax \equiv bx(mod\ n);$$

3 Vamos provar esse item usando indução sobre k: Para $k = 1$, nada temos a demonstrar.

Suponha que a proposição seja válida para algum $k \in \mathbb{N}$, vamos verificar a validade da proposição para $k+1$. Como $a \equiv b(mod\ n)$ e $a^k \equiv b^k(mod\ n)$ temos, pelo item 1, que $a^{k+1} \equiv b^{k+1}(mod\ n)$. Portanto, a proposição é válida para $k+1$. ■

Sabendo que a congruência é uma relação de equivalência, definimos então a classe de equivalência de $a \in \mathbb{Z}$ módulo n por:

$$\overline{a} = \{b \in \mathbb{Z} : a \equiv b(mod\ n)\}$$

Podemos agora obter um sistema com todos os possíveis restos da divisão euclidiana de a e b por n, dessa forma poderemos relacionar um elemento com sua classe de equivalência da seguinte forma:

Definição 13 *Um sistema reduzido de resíduos módulo n é um conjunto de números naturais* $r_1, \ldots r_s$ *tais que:*

1. *mdc*(r_i, n)*=1, para todo* $i = 1, \ldots, s$*;*

2. $r_i \neq r_j$ *mod (n), se* $i \neq j$*;*

3. *Para cada* $m \in \mathbb{N}$ *tal que mdc*(m, n)*=1, existe i tal que* $m \equiv r_i (mod\ n)$.

Pela Definição acima, um sistema de resíduos é constituído por uma quantidade finita de números naturais. A Definição a seguir fará uma relação entre n e o número de elementos do sistema de resíduos módulo n.

Definição 14 (Função de Euler) *Designamos por* $\phi(n)$ *o número de elementos de um sistema reduzido de resíduos módulo n,*

As observações a seguir são consequências imediatas da Definição 14.

Observação 2 $\phi(n) \leq n - 1$.

Observação 3 *Se p é um número primo, então* $\phi(p) = p - 1$.

Seja $\mathbb{Z}_p^*$, com p primo, o conjunto formado pelos elementos $\overline{a} \in \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$, com $\overline{a} = \{b \in \mathbb{Z} : a \equiv b(mod\ p)\}$, com $1 \leq a \leq p - 1$. Temos que todo $c \in \mathbb{Z}^*$ é congruente a um dos elementos $\overline{1}, \overline{2}, \ldots, \overline{p-1}$.

Definição 15 *Dados* $\overline{a}, \overline{b} \in \mathbb{Z}_p^*$*, então*

$$\overline{a} \oplus \overline{b} = \overline{a + b} \qquad e$$

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

Pelo item (1) do Teorema 12 temos que as operações de adição e multiplicação de números inteiros estão bem definidas no grupo $\mathbb{Z}_p^*$. A partir de agora trabalharemos com o grupo $\mathbb{Z}_p^*$ multiplicativo.

Afirmação 2 *$\overline{1}$ é o elemento neutro do grupo $\mathbb{Z}_p^*$ multiplicativo.*

Demonstração: Dado $\overline{a} \in \mathbb{Z}_p^*$, temos $\overline{a} \odot \overline{1} = \overline{a \cdot 1} = \overline{a}$ ■

Estamos "construindo" o grupo $\mathbb{Z}_p^*$, usando as Definições 5 e 11. Aparece a seguinte pergunta importante para nossos estudos "Será que existe $n \in \mathbb{Z}^*$ tal que $a^n \equiv 1(mod\ p)$?" O Teorema a seguir, conhecido como "Pequeno Teorema de Fermat", responde essa pergunta.

Teorema 16 (Pequeno teorema de Fermat): *Seja p um número primo e $a \in \mathbb{N}$ com $mdc(a,p)=1$, então $a^{p-1} \equiv 1(mod\ p)$*

Demonstração: Temos que

$$a^{p-1} \equiv 1(mod\ p) \Leftrightarrow p|a^{p-1} - 1 \Leftrightarrow p|a^p - a,\ pois\ mdc(a,p) = 1$$

Portanto para provar o Pequeno Teorema de Fermat, basta provar que $p|a^p - a$. Vamos usar indução sobre a para demonstrar essa proposição:

Para $a = 1$ o resultado é imediato.

Suponha que a proposição seja válida para a, vamos verificar a validade da proposição para $a + 1$:

$$(a+1)^p - (a+1) = a^p + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1} + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix} a + 1 - (a+1)$$

$$(a+1)^p - (a+1) = a^p - a + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1} + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix} a$$

é fácil ver que se p é primo, então $p \mid \begin{pmatrix} p \\ n \end{pmatrix}$, com $0 < n < p$, assim, pelo princípio da indução $p|a^p - a$, portanto, a proposição é válida para todo a natural. ■

A seguir veremos um corolário do Pequeno Teorema de Fermat que vai relacionar um elemento do grupo $\mathbb{Z}_p^*$ com um subgrupo cíclico dele.

Corolário 3.1 *Se $a \in \mathbb{Z}_p^*$. Se $0 < a < p$, então $\langle \overline{a} \rangle$ é um subgrupo cíclico de $\mathbb{Z}_p^*$.*

Podemos determinar uma relação entre a ordem do grupo multiplicativo $\mathbb{Z}_p^*$ e a Função de Euler de p.

Teorema 17 *Se p é um número primo, então $\mid \mathbb{Z}_p^* \mid = \phi(p)$*

Demonstração: Como p é primo temos pela, Definição 13, que

$$\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$

com isso, $\mid \mathbb{Z}_p^* \mid = p - 1$. Pela Definição 14

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

Portanto $\mid \mathbb{Z}_p^* \mid = \phi(p)$ ■

Veremos a seguir alguns exemplos de grupos $(\mathbb{Z}_p^*, \cdot)$:

Exemplo: $(\mathbb{Z}_3^*, \cdot) = \{\overline{1}, \overline{2}\}$: Calculando as potências de 2 que são congruentes a 1 ou 2 módulo 3 obtemos:

$$2^1 = 2 \equiv 2(mod\ 3)$$
$$2^2 = 4 \equiv 1(mod\ 3)$$
$$2^3 = 8 \equiv 2(mod\ 3)$$
$$2^4 = 16 \equiv 1(mod\ 3)$$
$$\vdots$$

Note que, pela Definição 4, $\overline{2}$ gera o grupo $\mathbb{Z}_3^*$. Portanto, $(\mathbb{Z}_3^*, \cdot)$ é um grupo cíclico. ⋄

Exemplo: $(\mathbb{Z}_5^*, \cdot) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$: Calculando as potências de 2 que são congruentes a 1, 2, 3 ou 4 módulo 5, obtemos:

$$2^1 = 2 \equiv 2(mod\ 5)$$
$$2^2 = 4 \equiv 4(mod\ 5)$$
$$2^3 = 8 \equiv 3(mod\ 5)$$
$$2^4 = 16 \equiv 1(mod\ 5)$$
$$\vdots$$

Calculando as potências de 3 que são congruentes a 1, 2, 3 ou 4 módulo 5 obtemos:

$$3^1 = 3 \equiv 3(mod\ 5)$$
$$3^2 = 9 \equiv 4(mod\ 5)$$
$$3^3 = 27 \equiv 2(mod\ 5)$$
$$3^4 = 81 \equiv 1(mod\ 5)$$

$$\vdots$$

Calculando as potências de 4 que são congruentes a 1, 2, 3 ou 4 módulo 5 obtemos:

$$4^1 = 4 \equiv 4(mod\ 5)$$

$$4^2 = 16 \equiv 1(mod\ 5)$$

$$4^3 = 64 \equiv 4(mod\ 5)$$

$$4^4 = 16 \equiv 1(mod\ 5)$$

$$\vdots$$

Note que $\langle\overline{2}\rangle = (\mathbb{Z}_5^*, \cdot)$ e $\langle\overline{3}\rangle = (\mathbb{Z}_5^*, \cdot)$, ou seja, $\overline{2}$ e $\overline{3}$ são geradores de $(\mathbb{Z}_5^*, \cdot)$. Portanto, $(\mathbb{Z}_5^*, \cdot)$ é um grupo cíclico. O grupo $\langle\overline{4}\rangle = \{\overline{1}, \overline{4}\}$ é um subgrupo de $(\mathbb{Z}_5^*, \cdot)$. $\diamond$

Note que nem todos os elementos de $\mathbb{Z}_p^*$ são geradores dele, vamos diferenciar esses elementos que são geradores a seguir.

Definição 18 *Dizemos que g é uma raiz primitiva de $\mathbb{Z}_p^*$ quando g é um gerador de $\mathbb{Z}_p^*$, ou seja,*

$$g \text{ é raiz primitiva de } \mathbb{Z}_p^* \Leftrightarrow \langle g\rangle = \mathbb{Z}_p^*$$

Exemplo: 2 e 3 são raízes primitivas de $\mathbb{Z}_5^*$ $\diamond$

Teorema 19 *g é raiz primitiva de $\mathbb{Z}_p^*$ se, e somente se, $\mid \langle\overline{g}\rangle \mid = \phi(p)$.*

Demonstração: ($\Rightarrow$) Se g é uma raiz primitiva de $\mathbb{Z}_p^*$, então, pela Definição 18, $\langle\overline{g}\rangle = \mathbb{Z}_p^*$, além disso, pelo Teorema 17, temos que $\mid \mathbb{Z}_p^* \mid = \phi(p)$. Portanto, $\mid \langle\overline{g}\rangle \mid = \phi(p)$.

($\Leftarrow$)$\mid \langle\overline{g}\rangle \mid = \phi(p) \Rightarrow \mid \langle\overline{g}\rangle \mid = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} \Rightarrow \mid \langle\overline{g}\rangle \mid = \mathbb{Z}_p^* \Rightarrow$ g é raiz primitiva de $\mathbb{Z}_p^*$ ■

Para determinarmos que o grupo $\mathbb{Z}_p^*$ é cíclico, basta encontrarmos uma raiz primitiva de $\mathbb{Z}_p^*$, ou seja, devemos encontrar um elemento $g \in \mathbb{Z}_p^*$ tal que $O(g) = \varphi(p)$.

Observação 4 *Na primeira seção deste capítulo foi demonstrado na Proposição 2 da página 6. Como $\mid \mathbb{Z}_p^* \mid = p - 1$, temos que: Se $O(g) = n$ e $m \in \mathbb{Z}$, então*

$$g^m \equiv 1(mod\ p) \Leftrightarrow m \mid n$$

Mas, pelo Pequeno Teorema de Fermat, sabemos que

$$g^{p-1} \equiv 1(mod\ p)$$

Portanto,

$$g^m \equiv 1(mod\ p) \Leftrightarrow p-1 = km$$

A observação acima funciona como critério para sabermos se um elemento é raiz primitiva de $\mathbb{Z}_p^*$. Para isso procedemos da seguinte forma. Para determinarmos se um elemento $g \in \mathbb{Z}_p^*$ é uma raiz primitiva de $\mathbb{Z}_p^*$, basta verificar se algum divisor de $p-1$ é congruente a 1 módulo p. Veremos a seguir alguns exemplos de como funciona esse critério.

Exemplo: Verificando se 2 é raiz primitiva de $\mathbb{Z}_7^*$: Como $\varphi(7) = 6$ e $6 = 2 \cdot 3$ temos que

$$2^2 = 4 \equiv 4(mod\ 7)$$

$$2^3 = 8 \equiv 1(mod\ 7)$$

Portanto, 2 não é raiz primitiva de $\mathbb{Z}_7^*$ $\diamond$

Exemplo: Verificando se 7 é raiz primitiva de $\mathbb{Z}_{11}^*$: Como $\varphi(11) = 10$ e $10 = 2 \cdot 5$ temos

$$7^2 = 49 \equiv 5(mod\ 11)$$

$$7^5 = 16807 \equiv 10(mod\ 11)$$

Portanto, 7 é raiz primitiva de $\mathbb{Z}_{11}^*$: $\diamond$

Agora vamos estudar um importante algoritmo que auxiliará nos cálculos de logaritmos Discretos. Esse algoritmo é conhecido como "Teorema Chinês dos Restos" e vai nos ajudar a resolver os sistemas de congruências que aparecerão nos cálculos do próximo Capítulo.

1.3 Teorema Chinês dos Restos

Segundo [5], No primeiro século da nossa era, o matemático chinês Sun-Tsu propôs o seguinte problema:

Qual é o número que deixa restos 2, 3 e 2 quando dividido, respectivamente, por 3, 5 e 7?

A resposta dada por Sun-Tsu para este problema foi 23.

Traduzindo em linguagem matemática, o problema de Sun-Tsu equivale a procurar as soluções do seguinte sistema de congruências:

$$X \equiv 2(mod\ 3)$$

$$X \equiv 3(mod\ 5)$$

$$X \equiv 2(mod\ 7).$$

Mais geralmente, resolveremos sistemas de congruências da forma:

$$a_1X \equiv b_1(mod\ m_1)$$

$$a_2X \equiv b_2(mod\ m_2)$$

$$\vdots$$

$$a_rX \equiv b_r(mod\ m_r).$$

Para que tal sistema possua solução, é necessário que $\text{mdc}(a_i; m_i) \mid b_i$, para todo $i = 1, \ldots, r$. Dessa forma o sistema acima é equivalente a um da forma

$$X \equiv c_1(mod\ n_1)$$

$$X \equiv c_2(mod\ n_2)$$

$$\vdots$$

$$X \equiv c_r(mod\ n_r).$$

Portanto vamos resolver um sistema de congruências encontrando a solução do sistema equivalente através do Teorema a seguir. O Teorema Chinês dos Restos é um algoritmo utilizado para calcular a solução de um sistema de congruências.

Teorema 20 (Teorema Chinês dos Restos) *O sistema*

$$X \equiv c_1(mod\ n_1)$$

$$X \equiv c_2(mod\ n_2)$$

$$\vdots$$

$$X \equiv c_r(mod\ n_r).$$

onde $mdc(n_i, n_j) = 1$*, para todo par* $n_i; n_j$ *com* $i \neq j$*, possui uma única solução módulo* $N = n_1n_2 \cdots n_r$*. Tal solução pode ser obtida como se segue:* $X = N_1y_1c_1 + \cdots + N_ry_rc_r$*; onde* $N_i = N/n_i$ *e* y_i *é solução de* $N_iY \equiv 1mod\ n_i,\ i = 1, \ldots, r$*.*

Demonstração: Primeiramente vamos provar que X é solução simultânea do sistema de congruência, como $n_i \mid N_j$, se $i \neq j$, e $N_i y_i \equiv 1(mod n_i)$, temos que

$$X = N_1 y_1 c_1 + \cdots + N_r y_r c_r \equiv N_i y_i c_i \equiv c_i (mod\ n_i)$$

Por outro lado, vamos mostrar que se x' é outra solução do sistema, então $x' \equiv x(mod\, n_1)$, $\forall i,\ i = 1, \ldots, r$. De fato. Como $\text{mdc}(n_i; n_j) = 1$, para $i \neq j$, segue-se que $mmc[n_1; \ldots; n_r] = n_1 \cdots n_r = N$ e, consequentemente, se $x \equiv x'(mod\, [n_1, \ldots, n_r]) \Rightarrow x \equiv x'(mod\ n_i), i = 1, \ldots, r$, temos que $x \equiv x'(mod\ N)$. ■

Vamos ver um exemplo da resolução de sistemas de congruências pelo Teorema Chinês dos Restos.

Exemplo: Qual o menor número natural que deixa restos 1, 3 e 5 quando dividido por 5, 7 e 9, respectivamente?

Solução: Para responder a pergunta acima, devemos resolver o sistema de congruências

$$x \equiv 1(mod\ 5)$$

$$x \equiv 3(mod\ 7)$$

$$x \equiv 5(mod\ 9).$$

Nesse caso, $N = 5 \cdot 7 \cdot 9 = 315$, logo $n_1 = 63,\ n_2 = 45,\ n_3 = 35$, com isso vamos resolver as seguintes congruências isoladamente:

$$63Y \equiv 1(mod\ 5) \Leftarrow y_1 = 2$$

$$45Y \equiv 1(mod\ 7) \Leftarrow y_2 = 5$$

$$35Y \equiv 1(mod\ 9) \Leftarrow y_3 = 8.$$

Portanto a solução módulo $N = 315$ é dada por:

$$X = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3 = 63 \cdot 2 \cdot 1 + 45 \cdot 5 \cdot 3 + 35 \cdot 8 \cdot 5 = 2201$$

Como $2201 \equiv 311(mod\ 315)$ concluímos que o número natural desejado é **311** ⋄

1.4 Personalidades Matemáticas

1.4.1 Leonhard Euler

Leonhard Euler (figura 1.1) foi, sem dúvida, um dos maiores e mais férteis matemáticos de todos os tempos. Ele nasceu na Suíça, perto da cidade de Basiléia, filho

Figura 1.1: Fonte:http://www-history.mcs.st-and.ac.uk/PictDisplay/Euler.html

de um modesto pastor protestante que nutria a esperança de que seu filho seguisse a mesma carreira.

Euler possuía uma grande facilidade para o aprendizado de línguas e uma prodigiosa memória, aliada a uma extraordinária habilidade para efetuar mentalmente contas complexas, habilidade esta que lhe seria muito útil no final de sua vida. Euler foi um dos matemáticos mais ativos da história. Ele escreveu livros sobre o cálculo das variações, no cálculo das órbitas planetárias, em artilharia e balística, em análise, sobre a construção naval e de navegação, sobre o movimento da lua. Depois de sua morte, em 1783 a Academia de São Petersburgo continuou a publicar trabalhos inéditos de Euler por mais de 50 anos mais.

1.4.2 Pierre de Fermat

Segundo [7], Pierre de Fermat (figura 1.2) era um advogado francês do Parlamento de Toulouse, na França, e um matemático amador, ele comunicava-se com outros matemáticos de sua época através de cartas, e nelas Fermat descrevia suas ideias, descobertas e até pequenos ensaios sobre assuntos de seu interesse, dentre os quais destacamos a teoria dos números. O Teorema 16, da página 11, foi enunciado por Fermat da seguinte forma: *Dado um número primo p, tem-se que p divide o número* $a^p - a$*, para todo* $a \in \mathbb{N}$.

Fermat é mais lembrado pelo o "Último Teorema de Fermat". Este teorema afirma que

$$x^n + y^n = z^n$$

Não tem soluções diferentes de zero inteiros para x, y e z, quando $n > 2$. Fermat escreveu, na margem da tradução de Arithmetica de Diofanto de Bachet. "Eu descobri uma prova verdadeiramente notável que esta margem é muito pequena para conter."

Acredita-se agora que a "prova" de Fermat estava errada embora seja impossível ter a certeza absoluta. A verdade da afirmação de Fermat foi provada em Junho de

Figura 1.2: Fonte:http://www-history.mcs.st-and.ac.uk/PictDisplay/Fermat.html

1993, pelo matemático britânico Andrew Wiles, mas Wiles retirou a reivindicação de ter uma prova, quando problemas surgiram mais tarde, em 1993. Em Novembro de 1994 Wiles novamente afirmou ter uma prova correta, que já foi aceita.

Tentativas frustradas de provar o teorema sobre um período de 300 anos levou à descoberta da teoria do anel comutativo e uma riqueza de outras descobertas matemáticas.

No próximo capítulo, adentramos no estudo do Logaritmo Discreto, cuja definição e propriedades são fundamentais no desenvolvimento de vários algoritmos de criptografia modernos.

Capítulo 2

Logaritmos Discretos

O estudo dos logaritmos discretos é essencial para entendermos a matemática por trás do algoritmo de criptografia ElGamal. Apresentaremos nesse capítulo a definição de logaritmos discretos, exemplos para calcular o logaritmo de um elemento no grupo $(\mathbb{Z}_p^*, \cdot)$, o problema do logaritmo discreto, algumas propriedades dos logaritmos que auxiliarão nos cálculos e como essas definições e propriedades facilitarão a explicação do algoritmo de criptografia ElGamal.

2.1 Logaritmos Discretos

Dado um elemento $\overline{a}$ do grupo cíclico $\mathbb{Z}_p^*$, (escreveremos $\overline{a} = a$) com $0 \leq a \leq p-1$, vimos na Definição 18 do capítulo anterior que a é uma raiz primitiva de $\mathbb{Z}_p^*$ quando a é um gerador de $\mathbb{Z}_p^*$. Desta forma, temos que qualquer elemento b de $\mathbb{Z}_p^*$ pode ser escrito na forma:

$$b = a^n, \text{ onde } n \in \mathbb{Z}$$

Precisamos encontrar uma forma de determinar o número n que satisfaz a equação acima e para isso vamos definir o logaritmo discreto de b na base a módulo p da seguinte forma:

Definição 21 *Dados $a, b \in \mathbb{Z}_p^*$, o* **logaritmo discreto** *de b na base a módulo p é o inteiro n, $0 \leq n \leq p-1$ para o qual $a^n \equiv b$, ou seja,*

$$\log_a b (mod\ p) = n \Leftrightarrow a^n \equiv b (mod\ p).$$

Usamos a seguinte notação para o logaritmo discreto:

$$\log_a b(mod\ p) = \log_{a;p} b$$

Note que a definição de logaritmos discretos é parecida com a definição de logaritmo de um número Real e positivo apresentada no Ensino Médio, em [4] logaritmo de um número real é definido da seguinte forma:

Definição 22 *O logaritmo de um número real e positivo b, na base a, positiva e diferente de 1, é o número x ao qual se deve elevar a para se obter b.*

$$\log_a b = x \Leftrightarrow a^x = b.$$

em que a é chamado de base do logaritmo, b é chamado logaritmando e x é chamado de logaritmo.

Daremos a mesma nomenclatura no logaritmo discreto de um **logaritmando** b na **base** a módulo p.

Quando p e a são números pequenos, o cálculo do logaritmo discreto é fácil, basta encontrar o expoente n que satisfaz a definição do logaritmo, como no exemplo a seguir:

Exemplo: Considerando o grupo cíclico $\mathbb{Z}_5^*$, e a base $a = 3$ basta calcular as potências de 3 que são congruentes a 1, 2, 3 ou 4 módulo 5 para obtermos os possíveis resultados de um número na base 3, ou seja:

$$3^1 = 3 \equiv 3(mod\ 5)$$

$$3^2 = 9 \equiv 4(mod\ 5)$$

$$3^3 = 27 \equiv 2(mod\ 5)$$

$$3^4 = 81 \equiv 1(mod\ 5).$$

Portanto, para qualquer $b \in \mathbb{Z}_5^*$, podemos encontrar seu logaritmo discreto comparando com os resultados encontrados acima, por exemplo: $\log_{3;5} 4 = 2$, pois $3^2 \equiv 4(mod\ 5)$ $\diamond$

Como consequência da definição de logaritmos discretos, temos que se a base não for uma raiz primitiva, então o logaritmo de um elemento do grupo cíclico pode não existir. Por exemplo, considerando o mesmo grupo $\mathbb{Z}_5^*$ temos $\log_4 2(mod\ 5) = \nexists$, pois não existe $n \in \mathbb{Z}$ tal que $4^n \equiv 2(mod\ 5)$. Para calcularmos o logaritmos discreto de um número não é preciso que a base seja uma raiz primitiva do grupo cíclico.

Teorema 23 *Se a base do logaritmo discreto for uma raiz primitiva de $\mathbb{Z}_p^*$, então o logaritmo discreto de qualquer elemento de $\mathbb{Z}_p^*$ existe.*

Demonstração: Dados $a, b \in \mathbb{Z}_p^*$, como a é uma raiz primitiva de $\mathbb{Z}_p^*$ temos, pela Definição 12, que $\exists n \in \mathbb{Z}$ tal que $b \equiv a^n (mod\ p)$, ou seja $\log_a b (mod\ p) = n$ ■

Como o logaritmo discreto de um elemento de $\mathbb{Z}_p^*$ sempre existe quando a base é uma raiz primitiva de $\mathbb{Z}_p^*$, vamos restringir nossos estudos a essas bases.

Para calcularmos o logaritmo discreto de um elemento $b \in \mathbb{Z}_p^*$ na base a, com a sendo uma raiz primitiva de $\mathbb{Z}_p^*$, precisamos montar uma tabela contendo as potências dessa raiz primitiva e a relação de congruência módulo p com b. Esse trabalho é muito demorado, por isso precisamos de um método prático e mais rápido para encontrar o resultado do logaritmo discreto de um elemento do grupo cíclico. Para isso vamos utilizar um algoritmo desenvolvido por Roland Silver, mas publicado pela primeira vez por Stephen Pohlig e Martin Hellman.

2.2 Algoritmo de Silver, Pohlig e Hellman

O algoritmo de Silver, Pohlig e Hellman foi desenvolvido para calcular o logaritmo discreto de um elemento em qualquer base que é gerador de um grupo cíclico $\mathbb{Z}_p^*$, com p primo.

Suponhamos que todos os fatores primos de $p-1$ sejam pequenos. Para simplificar, devemos supor que b é um gerador do grupo cíclico $\mathbb{Z}_p^*$.

Para cada primo q dividindo $p-1$, calcularemos as raízes q-ésimas da unidade

$$r_{q,j} = b^{\frac{j(p-1)}{q}}$$

para $j = 1, 2, \ldots, q$. Com nossa tabela de $\{r_{q,j}\}$ estaremos prontos para calcular o logaritmo discreto de qualquer $y \in \mathbb{Z}_p^*$. Note que se b é fixado, então este primeiro cálculo só precisa ser feito uma única vez, depois a mesma tabela é usada para qualquer y.

Nosso objetivo é determinar x, com $1 \leq x < p-1$, tal que $b^x = y$. Se

$$p - 1 = \prod_q q^a$$

é a fatoração em fatores primos de $p-1$, então é suficiente determinar

$$x (mod\ q^a)$$

para cada q dividindo $p-1$. Assim, x é unicamente determinado pelo Teorema Chinês dos Restos. Com isso, fixaremos um primo q dividindo $p-1$ e mostraremos como determinar

$$x(mod\ q^a).$$

Suponha que

$$x \equiv x_0 + x_1 q + \cdots + x_{\alpha-1} q^{\alpha-1} (mod\ q^\alpha)$$

com $0 \leq x_i < q$. Tomando a raiz q-ésima da unidade e sabendo que $y^{(p-1)} = 1$ e $y = b^x$, temos que

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

Com isso, comparamos $y^{\frac{p-1}{q}}$ com os $\{r_{q,j}\}$, $j = 1, 2, \ldots, q$, e igualamos x_0 com o valor de j com o qual $y^{\frac{(p-1)}{q}} = r_{q,j}$.

A seguir, para calcularmos x_1, substituímos y por

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

Então y_1 tem logaritmo discreto

$$x - x_0 \equiv x_1 + x_2 q + \cdots x_{\alpha-1} q^{\alpha-2} (mod\ p^\alpha).$$

Como y_1 é uma q-ésima potência temos que $y^{\frac{p-1}{q}}$ e

$$y_1^{\frac{p-1}{q^2}} = b^{\frac{(x-x_0)(p-1)}{q^2}} = b^{\frac{(x_1+x_2 q+\cdots x_{\alpha-1}q^{\alpha-2})(p-1)}{q}} = b^{\frac{x_1(p-1)}{q}} = r_{q,x_1}.$$

Desta forma, podemos comparar $y_1^{\frac{p-1}{q^2}}$ com $\{r_{q,j}\}, j = 1, 2, \cdots, q$, e igualamos x_1 com o valor de j para o qual $y_1^{\frac{p-1}{q^2}} = \{r_{q,j}\}$ e, assim sucessivamente, até obtermos $x_0, x_1, \ldots x_{\alpha-1}$.

Note que dependendo do valor de p é mais rápido calcular as potências de p para encontrarmos o logaritmo discreto de um número do que usar o Algoritmo de Silver, Pohlig e Hellman. Para entendermos o uso do Algoritmo de Silver, Pohlig e Hellman, vamos ver alguns exemplos.

Exemplo: Para começar vamos calcular o logaritmo discreto de 6 na base 7 em $\mathbb{Z}_{13}^*$ usando o algoritmo de Silver, Pohlig e Hellman.

Solução: Primeiro vamos calcular os fatores primos de 12,

$$12 = 4 \cdot 3 = 2^2 \cdot 3$$

Dessa forma os fatores primos de 12 são 2 e 3. Vamos agora determinar as raízes q-ésimas da unidade desses dois primos que dividem 12.

Para $p = 2$, temos:

$$\{r_{2,j}\} =< 7^{\frac{12}{2}} >=< 7^6 >$$
$$7^6 = 117649 = 13 \cdot 9049 + 12 \Rightarrow 7^6 \equiv 12(mod\ 13)$$
$$7^{12} \equiv 1(mod\ 13)[\text{pelo Teorema 16}].$$

Como $12 \equiv -1(mod\ 13)$, temos que $\{r_2, j\} = \{-1, 1\}$, nessa ordem.

Para $p = 3$, temos:

$$\{r_{3,j}\} =< 7^{\frac{12}{3}} >=< 7^4 >$$
$$7^4 = 2401 = 13 \cdot 184 + 9 \Rightarrow 7^4 \equiv 9(mod\ 13)$$
$$7^8 = 5764801 = 13 \cdot 443446 + 3 \Rightarrow 7^8 \equiv 3(mod\ 13)$$
$$7^{12} \equiv 1(mod\ 13)[\text{pelo Teorema 16}].$$

Portanto, $\{r_3, j\} = \{9, 3, 1\}$, nessa ordem.

Agora precisamos determinar x, tal que

$$6 \equiv 7^x(mod\ 13).$$

Para determinar x vamos realizar a seguinte etapa: para $p = 2$ temos que encontrar $x(mod\ 2)$ da seguinte forma:

$$6^{\frac{13-1}{2}} = 6^6 = 46656 = 13 \cdot 3588 + 12 \equiv -1(mod\ 13).$$

Dessa forma, como -1 ocupa a 1ª posição em $\{r_{2,j}\}$ temos que $x_0 = 1$.

Para $p = 3$ temos que encontrar $x(mod\ 3)$ repetindo o mesmo algoritmo:

$$6^{\frac{13-1}{3}} = 6^4 = 1296 = 13 \cdot 99 + 9 \equiv 9(mod\ 13).$$

Dessa forma como 9 ocupa a primeira posição em $\{r_{3,j}\}$ temos que $x_0 = 1$.

Agora vamos resolver o sistema de congruências:

$$x \equiv 1(mod\ 2)$$

$$x \equiv 1(mod\ 3).$$

É fácil ver que $x = 7$ é a solução do sistema acima, com isso temos

$$6 \equiv 7^7(mod\ 13).$$

Vamos verificar se a resposta está correta.

$$7^7 = 823543 = 13 \cdot 63349 + 6 \equiv 6(mod\ 13).$$

Portanto o algoritmo encontrou o logaritmo discreto conforme esperado. $\diamond$

Veremos a seguir outro exemplo do Algoritmo de Silver, Pohlig e Hellman.

Exemplo: Vamos calcular o logaritmo discreto de 17 na base 5 em $\mathbb{Z}_{23}^*$ usando o algoritmo acima:

Solução: Primeiro vamos calcular os fatores primos de 22,

$$q - 1 = 23 - 1 = 22 = 2 \cdot 11.$$

Vamos determinar as raízes q-ésimas da unidade desses dois primos que dividem 22.

Para $p = 2$, temos

$$\{r_{2,j}\} =< 5^{\frac{22}{2}} >=< 5^{11} >$$

$$5^{11} = 48828125 = 23 \cdot 2122961 + 22 \Rightarrow 5^{11} \equiv 22(mod\ 23)$$

$$5^{22} \equiv 1(mod\ 23)[\text{Pelo Teorema 16}].$$

Como $22 \equiv -1(mod\ 23)$, temos que $\{r_2, j\} = \{-1, 1\}$, nessa ordem.

Para $p = 11$, temos

$$\{r_{11,j}\} =< 5^{\frac{22}{11}} >=< 5^2 >$$

$$5^2 \equiv 2(mod\ 23)$$

$$5^4 \equiv 4(mod\ 23)$$

$$5^6 \equiv 8(mod\ 23)$$

$$5^8 \equiv 16(mod\ 23)$$

$$5^{10} \equiv 9(mod\ 23)$$

$$5^{12} \equiv 18(mod\ 23)$$

$$5^{14} \equiv 13(mod\ 23)$$

$$5^{16} \equiv 3(mod\ 23)$$

$$5^{18} \equiv 6(mod\ 23)$$

$$5^{20} \equiv 12(mod\ 23)$$

$$5^{22} \equiv 1(mod\ 23).$$

Portanto, $\{r_{11,j}\} = \{2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1\}$, nessa ordem. Agora precisamos determinar x, tal que

$$17 \equiv 5^x (mod\ 23).$$

Para determinar x vamos realizar a seguinte etapa: para $p = 2$ temos que encontrar $x(mod\ 2)$ da seguinte forma

$$17^{\frac{23-1}{2}} = 17^{11} = 34271896307633 = 1490082448157 \cdot 23 + 22 \equiv -1(mod\ 23).$$

Assim, como -1 ocupa a 1ª posição em $\{r_{2,j}\}$, temos que $x_0 = 1$.

Para $p = 11$ temos que encontrar $x(mod\ 11)$, repetindo o mesmo algoritmo

$$17^{\frac{23-1}{2}} = 17^2 = 289 \equiv 13(mod\ 23).$$

Assim, como 13 ocupa a 7ª posição em $\{r_{11,j}\}$, temos que $x_0 = 7$. Agora vamos resolver o sistema de congruências

$$x \equiv 1(mod\ 2)$$

$$x \equiv 7(mod\ 11).$$

E fácil ver que $x = 7$ é a solução do sistema acima, com isso temos

$$17 \equiv 5^7 (mod\ 23).$$

Portanto, o logaritmo discreto de 17 na base 5 em $\mathbb{Z}_{23}^*$ é **7**. $\diamond$

Note que se a decomposição em fatores primos de $p - 1$ tiver muitos termos, o uso do Algoritmo de Silver, Pohlig e Hellman para calcular o logaritmo discreto de um elemento se torna demorado, ou seja, a quantidade de fatores primos de $p - 1$ é diretamente proporcional ao tempo para realizar o cálculo do logaritmo discreto de um elemento do grupo cíclico $\mathbb{Z}_p^*$. Até o momento ninguém (nem os pesquisadores especializados) conseguiu encontrar um algoritmo rápido para calcular o logaritmo discreto de um elemento a do grupo cíclico $\mathbb{Z}_p^*$, esse problema é conhecido como **Problema do Logaritmo Discreto**.

Capítulo 3

Algoritmo e Criptografia

Faremos agora uma breve introdução histórica sobre Algoritmo e Criptografia, mostrando alguns exemplos. Depois mostraremos algoritmos de criptografia de chave pública para podermos entender como funciona o algoritmo de criptografia ElGamal, que será estudado no próximo capítulo.

3.1 Algoritmo e Criptografia

3.1.1 Algoritmo

Em [6], algoritmo é definido da seguinte forma:

> *Substantivo masculino*
> *1 Rubrica: matemática.*
> *sequência finita de regras, raciocínios ou operações que, aplicada a um número finito de dados, permite solucionar classes semelhantes de problemas*
> *2 Rubrica: informática.*
> *conjunto das regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas.*

Quando realizamos uma tarefa seguindo procedimentos pré-definidos, estamos utilizando um algoritmo, seja fazendo uma receita culinária ou até manter uma rotina diária de tarefas pessoais e profissionais, como ligar um computador pessoal, por exemplo. Geralmente realizamos essa tarefa da seguinte forma:
1º passo: ligar a "fonte de energia";

2º passo: ligar o "Desktop";
3º passo: ligar o "monitor".
Note que as etapas do algoritmo são importantes para sua realização. No exemplo citado acima não poderíamos ligar o "Desktop" sem primeiro ligar a "fonte de energia".

Os historiadores atribuem a origem da palavra *algoritmo* ao sobrenome, Al-Khwarizmi, do matemático persa do século IX Abu Jafar Mohamed ibn Musa al-Khwarizmi (figura 3.1). Suas obras foram traduzidas no ocidente cristão no século XII, tendo uma delas recebido o nome *Algorithmi de numero indorum*, sobre os algoritmos usando o sistema de numeração decimal (indiano).

Figura 3.1: Fonte:http://www.brasilescola.com/biografia/abu-jafar-mohamed-ibn-musa.htm

Na matemática, os algoritmos aparecerem por toda a história, os utilizados para realizar as operações básicas são os mais antigos e utilizados nosso dia-a-dia, dentre os quais destacamos o algoritmo para calcular o MDC de dois ou mais números desenvolvido por Euclides de Alexandria (figura 3.2), considerado o mais antigo da história.

Um estudante no Ensino Fundamental ou Médio depara-se com vários algoritmos durante sua vida, fora os já citados anteriormente. Podemos destacar aqueles que são utilizados diversas vezes na resolução de problemas no Ensino Fundamental e Médio. Veremos a seguir exemplos de algoritmos que os alunos aprendem no decorrer das séries que estudam.

Figura 3.2: Fontehttp://www.infoescola.com/biografias/euclides/

1. **ALgoritmo Euclidiano do MDC - Sexto Ano do Ensino Fundamental**

   O algoritmo é composto de uma tabela com 3 linhas, sendo a do meio composta pelos dois números e depois os restos da divisão euclidiana desses números e assim sucessivamente, a primeira linha é composta pelos resultados dessas divisões e a terceira linha é composta pelos restos das divisões, até chegar no número zero. Feito isso o mdc entre os dois números será o último número da segunda linha quando chegamos no resto zero.

   Exemplo: Para calcular mdc(143,17), fazemos

	8	2	2	3
143	17	7	3	**1**
7	3	1	0	

   Portanto, mdc(143,17)=1 $\diamond$

2. **Regra de Três Composta - Sétimo Ano do Ensino Fundamental**

   A regra de três composta é um algoritmo utilizado para resolver problemas que envolvem três ou mais grandezas, sejam elas diretamente ou inversamente proporcionais. O algoritmo é composto dos seguintes passos:

   1º passo : isolamos a grandeza que contém o termo desconhecido e ordenamos as demais grandezas;

   2º passo : verificamos se a grandeza do termo desconhecido é diretamente ou inversamente proporcional às demais grandezas proporcionais, e o faremos, sempre levando em conta que a grandeza não envolvida é constante;

3º passo : utilizamos as seguintes propriedades para encontrar o termo desconhecido:

I- Se uma grandeza X é diretamente proporcional a duas ou mais grandezas A, B, C, D, ... ela será diretamente proporcional ao produto das medidas dessas grandezas A, B, C, D, ...

II - Se uma grandeza X é diretamente proporcional a A, B, C, ... e inversamente proporcional a M, N, P, ..., ela será diretamente proporcional ao produto das medidas de A, B, C, ... pelo produto dos inversos das medidas de M, N, P, ...

Exemplo: *Para se alimentar 18 porcos por um período de 20 dias são necessários 360 kg de farelo de milho. Quantos porcos podem ser alimentados com 500 kg de farelo durante 24 dias?*

1º passo : isolando a grandeza que contém o termo desconhecido e ordenando as demais grandezas

número de porcos	tempo (dias)	quantidade de farelo (kg)
18	20	360
x	24	480

2º passo : verificando se a grandeza quantidade de porcos é diretamente ou inversamente proporcional às demais grandezas,

I - As grandezas número de porcos e tempo são inversamente proporcionais, já que, quanto mais porcos comerem menos tempo durará o estoque de farelo de milho.

II - As grandezas número de porcos e quantidade de farelo são diretamente proporcionais, já que, quanto mais porcos, mais farelo será necessário para alimentá-los.

3º passo : Como a grandeza quantidade de farelo é diretamente proporcional e a grandeza tempo é inversamente proporcional à grandeza quantidade de porcos, esta será diretamente proporcional ao produto das medidas quantidade de farelo e o inverso da medida que exprime o tempo. Assim, teremos

$$\frac{18}{x} = \frac{\frac{1}{20} \cdot 360}{\frac{1}{24} \cdot 480} \Rightarrow \frac{18}{x} = \frac{24 \cdot 360}{20 \cdot 480} \Rightarrow x = 20.$$

Portanto, podem ser alimentados 20 porcos. ◇

3. **Quadrado da Soma e da Diferença de Dois Termos - Oitavo Ano do Ensino Fundamental**

Um binômio elevado ao segundo expoente é desenvolvido utilizando o seguinte algoritmo:

1º passo: Calcula-se o primeiro monômio elevado ao expoente dois;

2º passo: Calcula-se o dobro do produto entre o primeiro monômio e o segundo monômio;

3º passo: Calcula-se o segundo monômio elevado ao expoente dois.

Exemplo: Desenvolvendo $(2x + 3y)^2$ temos:

1º passo

$$(2x)^2 = (2)^2(x)^2 = 4x^2$$

2º passo

$$2(2x)(3y) = 12xy$$

3º passo

$$(3y)^2 = (3)^2(y)^2 = 9y^2$$

Portanto o desenvolvimento é $4x^2 + 12xy + 9y^2$. $\diamond$

4. **- Fórmula de Báskara-Nono Ano do Ensino Fundamental**

Dada uma equação que pode ser escrita na forma reduzida

$$ax^2 + bx + c = 0, \text{com} \;\; a \neq 0. \tag{3.1}$$

Encontramos suas raízes usando um algoritmo conhecido como "fórmula de Báskara", seguindo os seguintes passos:

1º passo: determinamos os valores dos coeficientes a, b e c;

2º Passo: calculamos o valor do discriminante, representando pela letra grega Δ, usando a fórmula

$$\Delta = b^2 - 4 \cdot a \cdot c$$

3º passo: usamos a fórmula

$$x = \frac{-b \pm \sqrt{\Delta}}{2 \cdot a}$$

para determinar as duas possíveis raízes da equação 3.1, uma denominada x_1, usando o valor positivo de $\sqrt{\Delta}$, e a outra x_2 usando o valor negativo de $\sqrt{\Delta}$

Exemplo: Resolvendo a equação $x^2 - 5x + 6 = 0$ pela fórmula de báskara, obtemos:

1º passo Determinando os coeficientes:

$$a = 1; b = -5; c = 6$$

2º passo Calculando o discriminante:

$$\Delta = (-5)^2 - 4 \cdot (1) \cdot (6) = 25 - 24 = 1$$

2º passo encontrando as raízes:

$$x = \frac{-(-5) \pm \sqrt{1}}{2 \cdot (1)} = \frac{5 \pm 1}{2}$$

$$x_1 = \frac{5+1}{2} = \frac{6}{2} = 3 \text{ e } \; x_2 = \frac{5-1}{2} = \frac{4}{2} = 2$$

Portanto a solução da equação é o conjunto $S = \{2, 3\}$. $\diamond$

5. **Construção do gráfico de uma funçao do 1º grau - Primeiro Ano do Ensino Médio**

   Dada a função $f(x) = a \cdot x + b$. Para construir o gráfico da função, procedemos os seguintes passos:

   1º passo : calculamos os zeros da função usando a fórmula:

   $$x = -\frac{b}{a};$$

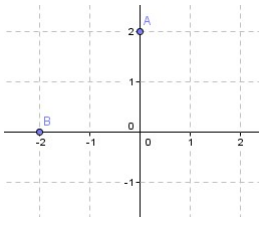
   2º passo : marcamos os pontos (x,0) e (0,b) no plano cartesiano;

   3º passo : traçamos uma reta que passa pelos pontos marcados no gráfico.

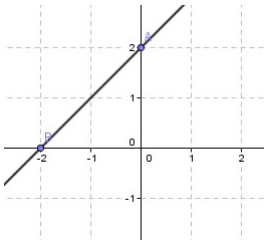
   Exemplo: *construir o gráfico da função* $f(x) = x + 2$

   1º passo : $x = -\frac{2}{1} = -2$

   2º passo :



   3º passo :



◇

6. **Cálculo do determinante de uma matriz de terceira ordem - Segundo Ano do Ensino Médio**

   1º passo : escrever à direita da matriz as duas primeiras colunas da mesma;

   2º passo : Somam-se então os produtos dos elementos das diagonais que partem de cima e da esquerda;

   3º passo : subtraem-se os produtos dos elementos das diagonais que partem de cima e da direita.

   Exemplo: *Calcular o determinante da matriz*

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 2 \\ 1 & 0 & 3 \end{pmatrix} :$$

   1º passo :

$$|A| = \begin{vmatrix} 1 & 2 & 3 & 1 & 2 \\ 0 & 2 & 2 & 0 & 2 \\ 1 & 0 & 3 & 1 & 0 \end{vmatrix}$$

   2º passo :

$$1 \cdot 2 \cdot 3 + 2 \cdot 2 \cdot 1 + 3 \cdot 0 \cdot 0 = 10;$$

   3º passo :

$$-1 \cdot 2 \cdot 3 - 0 \cdot 2 \cdot 1 - 3 \cdot 0 \cdot 2 = 6.$$

   Portanto o determinante da matriz A é 10-6=4. ◇

7. **Distância entre Dois Pontos - Terceiro Ano do Ensino Médio**

No plano cartesiano xy a distância entre os pontos $A = (x_A, y_A)$ e $B = (x_B, y_B)$ é determinada pelo algoritmo:

$$d_{A,B} = \sqrt{(x_B - x_A)^2 + (y_B - y_A)^2}$$

Exemplo: Para determinar a distância entre os pontos $A(0, 3)$ e $B(4, 0)$ usamos:

$$d_{A,B} = \sqrt{(4-0)^2 + (0-3)^2} = \sqrt{9+16} = \sqrt{25} = 5$$

Portanto a distância entre os pontos A e B é de 5 unidades de medida. $\diamond$

A linguagem computacional é uma linguagem binária que o computador utiliza para reconhecer e armazenar os dados. Por isso o computador utiliza um algoritmo que transforma todos os dados existentes nele para a linguagem binária. Por exemplo, para utilizar um editor de texto, como o que está sendo utilizado neste trabalho, o computador compila todos os caracteres digitados para a linguagem binária utilizando algoritmos que, devido a sua complexidade, não serão mostrados.

3.1.2 Criptografia

Quando queremos trocar informações sigilosas, precisamos escrevê-las de uma forma que só quem vai receber a informação entenda. Para fazê-lo, a pessoa pode utilizar uma linguagem que deve ser simples para ele mas para os outros é muito difícil de entender.

Segundo [6], criptografia é definida da seguinte forma:

> *Substantivo feminino*
> *1. conjunto de princípios e técnicas empregadas para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas; criptologia*
> *2. em operações políticas, diplomáticas, militares, criminais etc., modificação codificada de um texto, de forma a impedir sua compreensão pelos que não conhecem seus caracteres ou convenções.*

Temos que quanto maior a dificuldade de descobrir a criptografia utilizada, mais seguro é o algoritmo utilizado para escrevê-la. Quando descobrimos o algoritmo de criptografia, dizemos que "quebramos" esse algoritmo. Fazer isso é um trabalho muito difícil, dependendo do algoritmo. Note que quebrar um algoritmo de criptografia significa descobrir os segredos de uma pessoa ou empresa, senhas, contratos, transações, entre outras coisas, por isso os algoritmos de criptografia precisam ser seguros. Veremos a seguir alguns exemplos de algoritmos de criptografia que são fáceis de quebrar.

Leonardo da Vinci (figura 3.3) é considerado por vários o maior gênio da história, devido a sua multiplicidade de talentos para ciências e artes, sua engenhosidade e criatividade, além de suas obras polêmicas. O escritor americano Dan Brow (figura 3.4) escreveu em seu livro "O Código Da Vince" que quando Leonardo da Vinci escrevia seus projetos no seu diário ele usava um algoritmo bastante simples, bastava escrever as letras ao contrário, dessa forma quem pegasse seu diário não entendia o que estava lendo, mas para Leonardo da Vinci bastava colocar um espelho sobre o diário para ler o projeto desejado.

Figura 3.3: Fonte:http://www.leonardodavinci.net/images/leonardo-da-vinci.jpg

Figura 3.4: Fonte:http://blog.bookstellyouwhy.com/Portals/237126/images/dan-%20brown.jpg

Em outro livro escrito por ele, chamado "Fortaleza Digital", Dan Brow escreveu sobre outro algoritmo de criptografia muito simples: bastava escrever uma palavra usando a próxima letra do alfabeto de cada letra da palavra, por exemplo, para escrever o texto "matematica" era necessário escrever "nbufnbujdb".

Na área militar, a criptografia é bastante utilizada para trocar informações se-

cretas entre as tropas. A Segunda Guerra Mundial foi uma das que mais foram utilizados algoritmos de criptografia, eles serviram para organizar o Dia D sem que os alemães suspeitassem de nada, contribuindo assim para a vitória do bloco dos Aliados. A segurança do algoritmo de criptografia utilizado pelas forças armadas é de fundamental importância para o sucesso de uma campanha militar, as informações são trocadas constantemente e podem ser interceptadas pelas forças inimigas, por isso a utilização desses algoritmos foi muito difundido na área militar.

Com a aparição da internet, a troca de mensagens entre pessoas ou empresas passou a ser realizada de uma forma muito rápida e intensa, porém, essas mensagens podem ser interceptadas por qualquer pessoa com um pequeno conhecimento computacional. Por isso, foram desenvolvidos sistemas de criptografia, também conhecidos como "Criptossistemas", para que as informações fossem mantidas em segredo.

Daremos início agora ao estudo de alguns sistemas de criptografia que utilizam o conceito de "chave pública", também conhecidos como "algoritmos assimétricos". Esses criptossistemas são bastante utilizados no mundo digital por sua funcionalidade e dificuldade de serem quebrados.

3.2 Sistemas de Criptografia de chave pública

Os criptossistemas de chave pública apareceram para resolver o problema de segurança na troca de informações pela internet, principalmente os de autenticação e integridade. Eles propõem um modelo onde são utilizadas duas chaves, uma para cifrar e outra para decifrar as mensagens. Em um cenário típico, um emissor usa a chave pública do receptor para criptografar uma mensagem. Apenas o receptor possui a chave particular relacionada para descriptografar a mensagem. A complexidade da relação entre a chave pública e a chave particular significa que, contanto que as chaves tenham o comprimento necessário, é impraticável, em termos computacionais, determinar uma a partir da outra.

A ideia utilizada é simples, na troca de mensagens cada usuário possui um par de chaves, uma particular e outra pública, de tal forma que quando uma mensagem é cifrada pela chave pública ela só pode ser decifrada pela chave particular, em termos matemáticos, a chave pública é uma função $f(x)$ e a chave particular é a função inversa $f^{-1}(x)$ da chave pública. Esse esquema é ilustrado na figura 3.5.

Dessa forma, quando as chaves são conhecidas, as mensagens são decifradas de uma forma fácil e rápida, mas se não for conhecida uma das chaves, em especial a particular, a mensagem torna-se praticamente impossível de ser decifrada em tempo hábil. O tempo necessário para decifrar um criptossistema é determinado por [12] da seguinte forma:

Figura 3.5: Esquema do Algoritmo Assimétrico (construção do próprio autor)

1. Seja n o comprimento de entrada de um algoritmo A;
2. O algoritmo A é de tempo polinomial se a função $t(n)$ do tempo de execução no pior caso de A é tal que $t(n) = O(n^k)$ para um constante k;
3. O algoritmo A é de tempo exponencial se não existe constante k tal que $t(n) = O(n^k)$.

Conclui-se com isso que um criptossistema de tempo polinomial é mais fácil de quebrar do que o de tempo exponencial, porém o tempo necessário para quebrar um criptossistema de tempo polinomial pode ser tão grande que se torna praticamente impossível, até mesmo para um pesquisador especializado.

Os algoritmos de chave pública geralmente baseiam-se no "problema do logaritmo discreto" citado no final do segundo capítulo. Os pesquisadores Whitfield Diffie e Martin Hellman foram os primeiros a propor o modelo de criptografia de chave pública, em 1976. O criptossistema desenvolvido por eles será mostrado a seguir.

3.2.1 O Sistema Diffie-Hellman

Whitfield Diffie (figura 3.6) e Martin Hellman (figura 3.7) desenvolveram seu criptossistema utilizando o conceito do problema do logaritmo discreto citado no final do Capítulo 2, os dois propuseram que na troca de informações de dois usuários u_1 e u_2, onde cada um possui uma chave secreta k_{i1} e k_{i2}, respectivamente, dessa forma eles criarão uma chave particular k_{ij} da seguinte forma. Primeiramente eles devem escolher um parâmetros público, nesse caso um número primo p extremamente grande (com aproximadamente 100 dígitos) e um número q tal que

$$mdc(p, q) = 1.$$

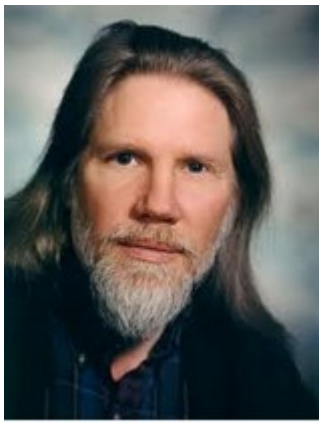


Figura 3.6:

Fonte:

http://www.enterprisemobilehub.com/sites/default/files/featured_img/whitdiffiephoto.jpg

Figura 3.7: Fonte:http://www-ee.stanford.edu/ hellman/

A seguir o usuário u_1 calcula

$$k_{c1} \equiv q^{k_{i1}} (mod\ p)$$

e envia k_{c1} para u_2, este por sua vez calcula

$$k_{c2} \equiv q^{k_{i2}} (mod\ p)$$

e envia k_{d2} para u_1. Finalmente eles calculam

$$k_{ij} \equiv q^{k_{i1} \cdot k_{i2}} (mod\ p)$$

$$\equiv k_{c1}^{i2}(mod\ p)$$
$$\equiv k_{c2}^{i1}(mod\ p).$$

Dessa forma, os dois usuários conseguem cifrar e decifrar a mensagem.

Para uma pessoa que não conhece as duas chaves particulares quebrar esse criptossistema, é preciso fazê-lo através de tentativa e erro, esse trabalho é dificultado ainda pelo fato do número primo possuir 100 dígitos ou mais.

Veremos agora um dos criptossistemas mais utilizados na atualidade, pela sua simplicidade e impossibilidade de ser quebrado até agora.

3.2.2 Criptosistema RSA

Figura 3.8: Fonte:http://www.umsl.edu/ siegelj/information_theory/RSA.jpg

Os professores do Instituto de Tecnologia de Massachusetts (*em inglês*, Massachusetts Institute of Technology, MIT) Ronald Rivest, Adi Shamir e Leonard Adleman (figura 3.8) criaram em 1978 o criptossistema RSA, iniciais dos sobrenomes dos três professores. Esse criptossistema é o mais utilizado no mundo e possui vários trabalhos explicando seu funcionamento. A ideia do Criptossistema é apresentada a seguir.

Cada usuário u_i escolhe dois números primos distintos extremamente grandes p_i e q_i e aleatoriamente um número t_i tal que

$$mdc(t_i, (p_i - 1)(q_i - 1)) = 1.$$

A seguir u_i calcula

$$n_i = p_i \cdot q_i.$$

Em seguida temos

$$\phi(n_i) = \phi(p_i)\phi(q_i) = n_i + 1 - (p_i + q_i)$$

e também

$$r_i \equiv t_i^{-1}(mod\ \phi(n_i)).$$

Note que

$$r_i \equiv t_i^{-1}(mod\ \phi(n_i)) \Leftrightarrow r_i t_i \equiv 1(mod\ \phi(n_i)).$$

Feito isso, o usuário u_i torna público a chave de codificação

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

e mantém a chave particular

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

Note que a chave particular depende de r_i e caso alguém queira descobrir por tentativas essa chave, terá que testar todos os possíveis restos da divisão de t_i^{-1} por n_i, por isso quanto maiores os números primos p_i e q_i mais difícil é descobrir a chave particular $k_{d,i} = (n_i, r_i)$.

Veremos agora outro criptossistema baseado em logaritmos discretos, o algoritmo de criptografia ElGamal. Faremos um estudo mais detalhado desse criptossistema, mostrando exemplos e apresentando as dificuldades em tentar quebrá-lo.

Capítulo 4

Algoritmo de Criptografia ElGamal

Figura 4.1: http://www.certicom.com/index.php/dr-taher-elgamal

O egípcio Taher ElGamal (figura 4.1) desenvolveu em 1984 seu criptossistema baseado no problema do logaritmo discreto, ou seja, ele baseou-se na dificuldade de calcular logaritmos discretos com elementos de um grupo cíclico finito G. Vimos que em 1976, Whitfield Diffie e Martin Helmann desenvolveram um criptossistema baseado no mesmo conceito, por isso a detentora da patente do criptossistema Diffie-Helmann reclamou os direitos para licenciar seu uso.

4.1 O Algoritmo de Criptografia ElGamal

Vamos mostrar como funciona esse criptossistema, explicando cada passo do algoritmo usando como base o artigo [2], escrito pelo próprio Taher ElGamal, e as notas de aula do professor Pedro Quaresma [9].

Para começar, o usuário A deve criar uma chave particular x_A e outra pública y_A para que o usuário B possa utilizar y_A para criptografar uma mensagem m e o usuário A descriptografar m usando x_A.

O usuário A cria a chave particular e a pública da seguinte forma:

1. A escolhe um número primo p de grande dimensão, dessa forma ele trabalhará com o grupo cíclico $\mathbb{Z}_p^*$;
2. Agora A escolhe $g \in \mathbb{Z}_p^*$, de preferência uma raiz primitiva desse grupo cíclico;
3. A chave particular de A é o número $k \in \mathbb{Z}$ tal que $1 \leq k \leq p-1$;
4. A calcula
$$r \equiv g^k (mod\ p). \tag{4.1}$$
Dessa forma A cria a chave pública (r, g, p).

Observação 5 *Note que para algum intruso determinar a chave particular k ele deve calcular*

$$k = log_{g;p} r.$$

É justamente nesse ponto que aparece o "problema do logaritmo discreto".

Para o usuário B criptografar uma mensagem m ele utiliza a chave pública (r, g, p) e realiza os seguintes passos:

1. B escolhe um inteiro $b, 1 \leq b \leq p-2$ para ser sua chave particular e calcula
$$s \equiv g^b (mod\ p); \tag{4.2}$$
2. Para criptografar a mensagem m, B calcula:
$$\gamma \equiv m \cdot r^b (mod\ p); \tag{4.3}$$
3. A mensagem cifrada é representado pelo par (s, γ).

Quando A recebe o par (s, γ) de B, segue o seguinte procedimento para descriptografar a mensagem:

1. A Calcula
$$y \equiv s^{p-1-k} (mod\ p). \tag{4.4}$$
Note que para isso ele usa sua chave particular k;
2. Para descriptografar a mensagem A calcula
$$m \equiv y \cdot \gamma (mod\ p). \tag{4.5}$$

Com isso A recupera a mensagem m.

4.1.1 Verificando a autenticidade do algoritmo

Vamos verificar agora a autenticidade do algoritmo de criptografia ElGamal. para isso, vamos mostrar que a equação 4.5 é satisfeita. De 4.4 temos que

$$y \equiv s^{p-1-k}(mod\ p) \Rightarrow y \equiv s^{p-1} \cdot s^{-k}. \tag{4.6}$$

Pelo Teorema 16 na página 11 temos que

$$s^{p-1} \equiv 1(mod\ p)$$

e por 4.2 podemos escrever 4.6 da seguinte forma:

$$y \equiv g^{-bk}(mod\ p). \tag{4.7}$$

Agora por 4.3 podemos escrever 4.5 da seguinte forma:

$$m \equiv m \cdot r^b \cdot g^{-bk},$$

mas por 4.1, temos

$$m \equiv m \cdot g^{bk} \cdot g^{-bk}(mod\ p) \Rightarrow m \equiv m(mod\ p).$$

Veremos a seguir um exemplo numérico explicando os passos citados no Algoritmo de ElGamal. Para simplificar as contas trabalharemos com um número primo pequeno.

Exemplo: Trocando uma mensagem usando o Criptossistema ElGamal

Vamos começar escolhendo o número primo $p = 29$, dessa forma iremos trabalhar com o grupo $\mathbb{Z}_{29}^* = \{1, 2, 3, \ldots, 28\}$, escolhemos agora um elemento desse grupo, por exemplo $g = 3$. Vamos utilizar o número 20 como mensagem m a ser assinada.

O usuário A escolhe um número para ser sua chave particular, por exemplo $k = 10$ e realiza o seguinte cálculo:

$$r = g^k(mod\ p) = 3^{10}(mod\ 29) = 5$$

Com isso o usuário A cria a chave pública $(5, 3, 29)$.

O usuário B escolhe outro número para ser sua chave particular, por exemplo $b = 13$, e calcula:

$$s = 3^{13}(mod\ 29) = 19$$

A mensagem $m = 20$ é criptografada por B da seguinte forma:

$$\gamma = 20 \cdot 5^{13}(mod\ 29) = 4$$

Com isso o usuário B manda a mensagem criptografada para A através do par $(s, \gamma) = (5, 4)$.

A mensagem é então descriptografada pelo usuário A fazendo primeiro

$$y \equiv s^{p-1-k}(mod\ 29) = 19^{29-1-10}(mod\ 29) = 19^{18}(mod\ 29) = 5$$

Depois

$$m = y \cdot \gamma(mod\ 29) = 5 \cdot 4(mod\ 29) = 20(mod\ 29) = 20.$$

Dessa forma a mensagem criptografa e descriptografa foi transmitida utilizando o criptossistema ElGamal. $\diamond$

4.2 Possíveis Ataques ao Criptossistema

No mesmo trabalho [2], ElGamal mostrou alguns dos possíveis ataques que alguém pode realizar para quebrar seu criptossistema. Eles dividem-se em dois grupos:

1. Recuperar a chave particular x_A;
2. Forjar assinaturas sem recuperar a chave particular x_A.

4.2.1 Recuperando a chave particular x_A

Dados $\{m_i : i = 1, 2, \ldots i\}$ documentos, em conjunto com as assinaturas correspondentes $\{(s_i, \gamma_i) : i = 1, 2, \ldots, i\}$, um intruso pode tentar resolver i equações da forma (4.1). Temos que existem $i + 1$ incógnitas (uma vez que cada assinatura utiliza uma diferente chave particular b_i), o sistema de equações é indeterminado e o número de soluções é grande. A razão é que para cada valor de k origina uma solução para os b_i de um sistema de equações lineares, com uma matriz diagonal de coeficientes que irão resultar. Uma vez que p é escolhido para ser um número muito grande de caracteres, recuperar k requer um número exponencial de pares mensagens-assinatura.

Tentar resolver equações da forma (4.1) é sempre equivalente ao cálculo de logaritmos discretos sobre $\mathbb{Z}_p^*$.

Se uma chave particular k é usada duas vezes na assinatura, o sistema de equações torna-se possível e determinado e a mensagem m pode ser recuperada. Assim, para o sistema ser seguro, qualquer valor de k não pode ser usado mais de uma vez. Esse fato contribuiu para que o criptossistema ElGamal fosse considerado fácil de quebrar.

4.2.2 Forjando assinaturas sem recuperar a chave particular

Dado um documento m, um falsificador pode tentar encontrar (s, γ) de tal modo que (4.5) é satisfeita. Se $s \equiv g^j \ (mod\ p)$ é fixado para algum j escolhido aleatoriamente, então o cálculo de γ é equivalente a resolver o problema do logaritmo discreto sobre $\mathbb{Z}_p^*$.

Se o falsificador fixa γ primeiro, então s pode ser calculado a partir da equação

$$y^r r^s \equiv A \ (mod\ p) \tag{4.8}$$

Resolver (4.8) para s não é fácil, provou-se ser pelo menos tão difícil quanto resolver o problema do logaritmo discreto, mas acredita-se que não é possível resolver (4.8) em tempo polinomial.

Outra forma de atacar o criptossistema é tentar resolver (4.5) para ambos s e γ simultaneamente, mas ainda não apareceu um algoritmo eficiente para fazer isso em tempo polinomial.

Com isso concluímos a abordagem matemática do criptossistema ElGamal.

No próximo capítulo apresentaremos uma sequência de atividades que os professores do 1º ano do Ensino Médio podem trabalhar em sala de aula. Entre eles apresentamos outro exemplo do Criptossistema de ElGamal que pode ser trabalhado com estudantes desse nível de ensino.

Capítulo 5

Atividades para sala de aula

Neste capítulo apresentamos uma sequência de atividades didáticas, que podem ser utilizadas pelos professores de matemática em sala de aula, para estimular os alunos da 1º ano do Ensino Médio ao aprendizado de teoremas e definições complexos do Ensino Superior. Através de algoritmos simples tentamos incentivar aqueles alunos que desejam seguir com os estudos da matemática no Ensino Superior, bem como mostrar o criptossistema ElGamal, com um exemplo simples para os alunos que se interessam pela linguagem computacional, ou aqueles que gostariam de entender o método utilizado na troca de mensagens particulares criptografadas.

5.1 Algoritmos para aprender Teoremas e Definições

5.1.1 Atividade 1 - Determinando uma raiz primitiva de $\mathbb{Z}_p^*$

No primeiro Capítulo deste trabalho mostramos algumas propriedades dos grupos cíclicos $\mathbb{Z}_p^*$. Nessa atividade propomos um algoritmo simples que "encontra" os elementos desse grupo cíclico. Para facilitar o entendimento da mesma, não utilizaremos a linguagem usada no trabalho, mas uma linguagem mais simples. Para isso usaremos cálculos de potenciação e divisão de números naturais.

Atividade

Verificar se as potências de 3 quando divididas por 7 determinam todos os possíveis restos da divisão de um número natural por 7. Primeiro vamos calcular algumas potências de 3. Para isso propomos a utilização de uma calculadora científica (figura

5.1) disponível na internet pelo site *http://www.calculadoraonline.com.br/cientifica* para facilitar as contas. Serão utilizados os dois botões assinalados na figura abaixo.

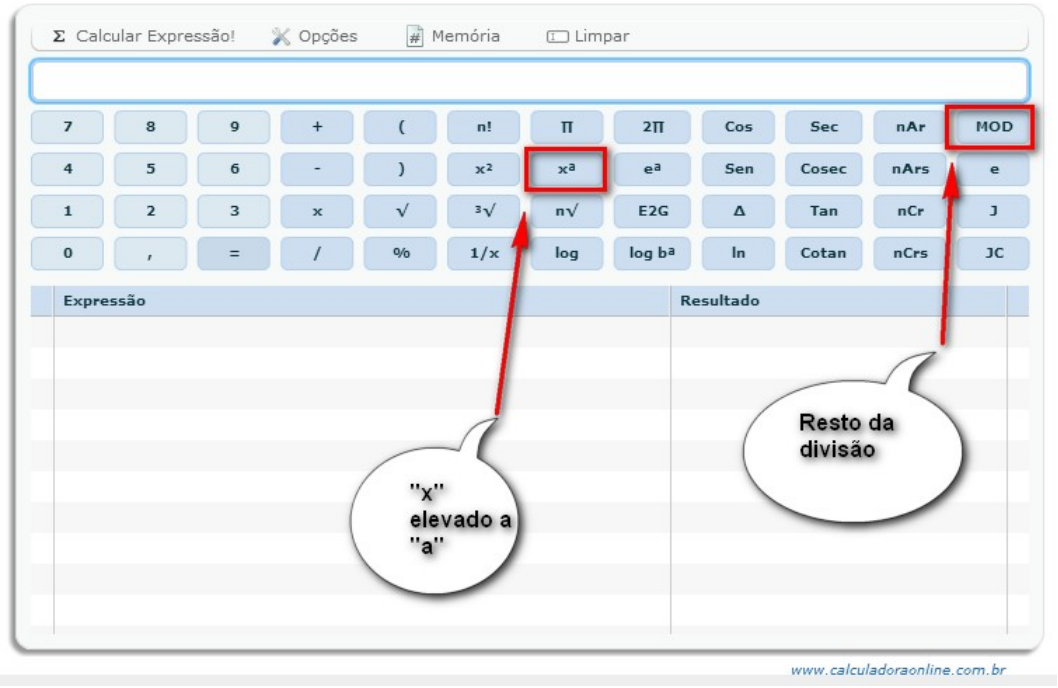


Figura 5.1: Calculadora Científica

Primeiro apertamos o botão destacado acima x^a ("x" elevado a "a") para calcular potências depois apertamos no 3 e finalmente no número que representa o expoente. Encontramos dessa forma os seguintes resultados:

$$3^1 = 3$$
$$3^2 = 9$$
$$3^3 = 27$$
$$3^4 = 81$$
$$3^5 = 243$$
$$3^6 = 729$$
$$3^7 = 2187$$
$$3^8 = 6561$$
$$3^9 = 19683$$

$$3^{10} = 59049$$
$$3^{11} = 177147$$
$$3^{12} = 531441.$$

Agora, apertando no outro botão destacado *mod* (Resto da divisão), calculamos com isso os restos da divisão de cada resultado por 7, obtemos com isso os seguintes resultados:

$$3(mod7) = 3$$
$$9(mod7) = 2$$
$$27(mod7) = 6$$
$$81(mod7) = 4$$
$$243(mod7) = 5$$
$$729(mod7) = 1$$
$$2187(mod7) = 3$$
$$6561(mod7) = 2$$
$$19683(mod7) = 6$$
$$59049(mod7) = 4$$
$$177147(mod7) = 5$$
$$531441(mod7) = 1.$$

A partir daí, o professor consegue mostrar que os próximos números irão repetir-se na ordem {3,2,6,4,5,1}, ou seja, os números repetem-se de forma "cíclica" e esses números são todo os possíveis restos da divisão euclidiana de um número natural por 7. Dessa forma o aluno pode aprender que as potências de 3 "determinam" todos os possíveis restos da divisão euclidiana de um número natural por 7 e esses números são determinados numa determinada ordem.

Com base no exemplo acima o professor pede aos alunos para fazer o seguinte exercício:

1. Verificar se as potências de 5, quando divididos por 7, determinam todos os possíveis restos dessa divisão euclidiana;

2. fazer uma tabela contendo as potências de 5 e os restos da divisão euclidiana dessas potências por 7;

3. Existem números naturais entre 1 e 7 cujas suas potências não determinam todos os possíveis restos da divisão euclidiana por 7? Quais são esses números?

Objetivo Geral

Apresentar teoremas e definições abstratas aos alunos do Ensino Fundamental e Médio através de cálculos básicos e incentivar o estudo da matemática do Ensino Superior.

Objetivos Específicos

- Calcular as potências de um número natural;
- Determinar o resto da divisão euclidiana entre dois números naturais;
- Reconhecer o comportamento cíclico de determinados conjuntos numéricos quando utilizamos algumas operações básicas;
- Construir tabelas com os dados apresentados;

Público Alvo

Estudantes do 1º ano do Ensino Médio, segundo os Parâmetros Curriculares Nacionais (PCN).

Pré-requisitos

Os alunos deverão saber usar o algoritmo euclidiano da divisão para determinar o resto da divisão entre dois números naturais, bem como calcular as potências de um número natural.

Materiais Utilizados

Os materiais utilizados nessa atividade são lápis, borracha, folha contendo a atividade, um computador com acesso a internet para acessar o site ou uma calculadora científica, e um projetor multimídia (datashow) para o docente mostrar como utilizar a calculadora científica para realizar os cálculos.

Recomendações Metodológicas

Esta atividade será aplicada num laboratório de informática com acesso a internet ao final do conteúdo de potenciação. Os alunos responderão as atividades em dupla e, posteriormente, se reunirão com os demais colegas para discutir os resultados obtidos. Ao término da discussão, o docente responderá a atividade ou poderá

propor aos alunos responderem com o auxílio do datashow.

Dificuldades Previstas

As dificuldades, que poderão surgir ao longo desta atividade, são aquelas referentes ao assunto divisão de números naturais, pois estudos comprovam a dificuldades dos alunos em todo o país com relação a esse conteúdo. O professor ao andar pelo laboratório pode ver o andamento das atividades e poderá ajudar os alunos que apresentarem essa dificuldade.

Possíveis Continuações ou Desdobramentos

O docente poderá utilizar outros valores para o número primo e a base da potência. Assim como optar por não usar a calculadora científica para que os alunos façam os cálculos no papel disponibilizado no material de apoio.

5.1.2 Atividade 2 - Calculando Logaritmos Discretos

No segundo Capítulo deste trabalho mostramos como calcular logaritmos discretos no grupo cíclico $\mathbb{Z}_p^*$. Nessa atividade propomos o cálculo do logaritmo discreto de um número b na base $a; p$, ou seja

$$log_{a;p}b$$

Atividade
Calcular $log_{2;13}7$. Realizar esse cálculo é o mesmo que determinar x tal que $2^x \equiv 7(mod\ 13)$. Primeiro deve-se calcular as potências de 2^1 até 2^{12}.

$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8$$
$$2^4 = 16$$
$$2^5 = 32$$
$$2^6 = 64$$
$$2^7 = 128$$
$$2^8 = 256$$
$$2^9 = 512$$

$$2^{10} = 1024$$
$$2^{11} = 2048$$
$$2^{12} = 4096.$$

Agora determinando os restos da divisão dos resultados acima por 13, obtemos os seguintes valores:

$$2 \equiv 2(mod\ 13)$$
$$4 \equiv 4(mod\ 13)$$
$$8 \equiv 8(mod\ 13)$$
$$16 \equiv 3(mod\ 13)$$
$$32 \equiv 6(mod\ 13)$$
$$64 \equiv 12(mod\ 13)$$
$$128 \equiv 11(mod\ 13)$$
$$256 \equiv 9(mod\ 13)$$
$$512 \equiv 5(mod\ 13)$$
$$1024 \equiv 10(mod\ 13)$$
$$2048 \equiv 7(mod\ 13)$$
$$4096 \equiv 1(mod\ 13).$$

A partir daí, o professor consegue mostrar que $log_{2;13}7 = 11$, pois $2^{11} \equiv 7(mod\,13)$.

Com base no exemplo acima o professor pede aos alunos para fazer o seguinte exercício:

1. Utilizando o esquema de flechas represente por meio de diagramas o logaritmo discreto de cada um dos números naturais menores do que 13 na base 2 com relação ao resto da divisão euclidiana por 13;

2. Verifique quais propriedades dos logaritmos de um número real são válidas para os logaritmos discretos tendo como base $log_{2;13}b$;

3. Se mudarmos a base do logaritmo discreto, o logaritmo de um número pode não existir. Mostre um exemplo de um número que não possui logaritmo discreto numa determinada base.

Objetivo Geral

Apresentar teoremas e definições abstratas aos alunos do Ensino Fundamental e Médio através de cálculos básicos e incentivar o estudo da matemática do Ensino Superior.

Objetivos Específicos

- Calcular o logaritmo discreto de um número b na base a com relação ao resto da divisão euclidiana de um número por um número primo p;
- Determinar o resto da divisão euclidiana entre dois números naturais;
- Retomar a ideia de diagramas por meio do esquema de flechas;
- Identificar quais propriedades os logaritmos discretos possuem;
- Relacionar a existência do logaritmo discreto de um número com o fato das potências da base determinarem todos os possíveis restos da divisão euclidiana de um número por outro;

Público Alvo

Estudantes do 1º ano do Ensino Médio, segundo os Parâmetros Curriculares Nacionais (PCN).

Pré-requisitos

Essa atividade deve ser realizada após a primeira atividade proposta anteriormente, portanto os pré-requisitos dela são os mesmos. Eles deverão saber também as propriedades do logaritmo de um número real.

Materiais Utilizados

Os materiais utilizados nessa atividade são lápis, borracha e folha contendo a atividade. O docente pode utilizar um computador com acesso a internet para acessar o site da calculadora científica e facilitar alguns cálculos.

Recomendações Metodológicas

Esta atividade será aplicada em sala de aula ao final do conteúdo de função logarítmica. Os alunos responderão as atividades em dupla e, posteriormente, se reunirão

com os demais colegas para discutir os resultados obtidos. Ao término da discussão, o docente responderá a atividade ou poderá propor aos alunos responderem na lousa.

Dificuldades Previstas

As dificuldades, que poderão surgir ao longo desta atividade, são aquelas referentes ao assunto função logarítmica e divisão de números naturais, pois estudos comprovam a dificuldades dos alunos em todo o país com relação a esses conteúdos. O professor ao andar pela sala e ver o andamento das atividades poderá ajudar os alunos que apresentarem essa dificuldade.

Possíveis Continuações ou Desdobramentos

O docente poderá utilizar outros valores para o número primo e a base do logaritmo. Dependendo do número primo escolhido, recomendamos o uso do algoritmo de Silver, Pohlig e Hellman na Seção 2.2 página 21. Ele pode também utilizar a primeira atividade proposta nesse capítulo para familiarizar o aluno com alguns cálculos e definições que serão realizados.

5.1.3 Atividade 3 - O Criptossistema ElGamal em sala de aula

No quarto Capítulo deste trabalho apresentamos o "Algoritmo de Criptografia ElGamal" para criptografar e descriptografar mensagens. Nessa atividade propomos um exemplo de como podemos utilizar esse algoritmo.

Atividade

Dois alunos A e B precisam trocar uma senha numérica via mensagem que será criptografada e descriptografada por eles. Iremos utilizar o número primo $p = 31$ e o número $g = 3$ como sendo a base das potências.

O aluno A escolhe um número positivo $k < 31$, por exemplo $k = 17$, e realiza o seguinte cálculo com o auxílio de uma calculadora:

$$r = g^k (mod\ p) = 3^{17} (mod\ 31) = 22$$

Dessa forma ele cria a cria a tripla ordenada $(r, g, p) = (22, 3, 31)$.

O aluno B escolhe um número positivo $b < 31$, por exemplo $b = 15$, e realiza o seguinte cálculo com o auxílio de uma calculadora:

$$s = g^b (mod\ p) = 3^{15} (mod\ 31) = 30$$

Agora para o aluno B criptografar a senha $j = 9$ usando a chave pública ele realiza o seguinte cálculo:

$$\gamma = j \cdot r^b (mod\ 31) = 9 \cdot 22^{15} (mod\ 31) = 22$$

O aluno B envia o par ordenado $(s, \gamma) = (30, 22)$ ao aluno A que realiza os seguintes cálculos para descriptografar a mensagem:

$$y = s^{p-1-a} (mod\ p) = 30^{31-1-17} (mod\ 31) = 30$$

A mensagem é então descriptografada fazendo:

$$j = y \cdot \gamma (mod\ 31) = 22 \cdot 30 (mod\ 31) = 660 (mod\ 31) = 9$$

Dessa forma o aluno A determina a senha $j = 9$ do aluno B.

Objetivo geral

Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a divisão e potenciação de números inteiros.

Objetivos específicos

1. Calcular o logaritmo discreto de um número b na base a com relação ao resto da divisão euclidiana de um número por um número primo p;
2. Determinar o resto da divisão euclidiana entre dois números naturais;

Público Alvo

Estudantes do 1º ano do Ensino Médio, segundo os Parâmetros Curriculares Nacionais (PCN).

Pré-requisitos

Os alunos deverão conhecer o algoritmo da divisão de Euclides, a definição e propriedades das potências de números naturais e a definição e obtenção de números primos.

Materiais Utilizados

Os materiais utilizados nesta atividade são lápis, borracha, calculadora científica e a folha contendo a atividade.

Recomendações Metodológicas

Esta atividade será aplicada em sala de aula ao final do conteúdo de potenciação para a verificação da aprendizagem dos alunos com relação a esse conteúdo. Os alunos deverão formar duplas para verificar, utilizando a calculadora para o cálculo de potências, se conseguiram chegar a mesma chave e codificar e decodificar as mensagens transmitidas. Ao final desta atividade o professor deverá discutir os resultados obtidos com os discentes, verificando se as mensagens foram trocadas com êxito.

Dificuldades previstas

As dificuldades, que poderão surgir ao longo desta atividade, são aquelas referentes ao assunto divisão de números naturais. O professor ao andar pela sala e ver o andamento das atividades poderá ajudar os alunos percebendo essa dificuldade.

Possíveis Continuações ou Desdobramentos

O docente poderá utilizar outros valores para o número primo e a base da potência, bem como mudar a mensagem utilizada na codificação e decodificação.

Referências Bibliográficas

[1] Coutinho, S. C. *Criptografia*, Rio de Janeiro: Série Computação e matemática, IMPA; (2003).

[2] ElGamal, Taher, *A Public Key Cryptosystem And A Signature Scheme Based On Discrete Logarithms*, IEEE Transactions on information, v. 31, p. 473-481 (1984) Disponível em: http://groups.csail.mit.edu/cis/crypto/classes/6.857 /papers/elgamal.pdf. Acesso em: 20 janeiro 2013.

[3] Garcia, Arnaldo, *Elementos da Algebra/* Arnaldo Garcia, Yves Lequain. 5. ed. Rio de Janeiro : IMPA, (2008).

[4] Giovanni, José Ruy, *Matemática Fundamental, 2º grau: Volume Único/* José Ruy Giovanni, José Roberto Bonjorno, José Ruy Giovanni Jr - São Paulo: FTD, (1994).

[5] Hefez, Abramo, *Elementos de Aritmética*, Rio de Janeiro, SBM, (2011).

[6] Houaiss, Antonio, *Dicionário Houaiss de língua portuguesa*, editora Objetiva LTDA, (2009).

[7] O'Connor, J J e Robertson, E F. *Pierre de Fermat* (1996). Disponível em: http://www-history.mcs.st-and.ac.uk/Biographies/Fermat.html. Acesso em 22 de agosto 2013.

[8] O'Connor, J J e Robertson, E F. *Leonhard Euler* (1998). Disponível em: http://www-history.mcs.st-and.ac.uk/Biographies/Euler.html. Acesso em 22 de agosto 2013

[9] Quaresma, Pedro, *Introdução às Cifras de Chave Pública e Cifra RSA, Capítulo VI*(2012), Notas de Aula, Disponível em: http://www.mat.uc.pt/ pedro/lectivos/CodigosCriptografia1213/apontamentos133a180.pdf. Acesso em: 21 Janeiro 2013.

[10] Rezende, Pedro Antônio Dourado de, *Criptografia e Segurança na Informática*, Notas de aula, (1998), Brasília: Universidade de Brasília. Disponível em: http://www.cic.unb.br/docentes/pedro/segdados_files/ CriptSegD.pdf . Acesso em: 20 janeiro 2013.

[11] Silva, Antônio de Andrade, *Números, Relações e Criptografia.* Departamento de Matemática - UFPB.

[12] SOUZA, Raimundo Cândido, *CRIPTOGRAFIA DE CHAVE PÚBLICA: ALGORITMOS QUE POSSIBILITAM A CRIAÇÃO DE CHAVE ASSIMÉTRICA*, Trabalho de Conclusão de Curso, (2005), Brasília: Universidade Católica de Brasília. Disponível em: http://www.ucb.br/sites/100/103/TCC/22005/ RaimundoCandidodeSousa.pdf. Acesso em: 21 janeiro 2013.