CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

Ana Carolina Sakurai Ferreira

CRIPTOGRAFIA DE CHAVE PÚBLICA-PRIVADA: RSA E CURVAS ELÍPTICAS

Maringá

2019

Ana Carolina Sakurai Ferreira

CRIPTOGRAFIA DE CHAVE PÚBLICA-PRIVADA: RSA E CURVAS ELÍPTICA

Trabalho de Conclusão de Curso apresentado ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.
Área de concentração: Matemática.

Orientadora: Profa. Dra. Claudete Matilde Webler Martins.
Coorientador: Prof. Dr. Rodrigo Martins.

Maringá

2019

Dados Internacionais de Catalogação-na-Publicação (CIP)
(Biblioteca Central - UEM, Maringá - PR, Brasil)

F383c

Ferreira, Ana Carolina Sakurai
Criptografia de chave pública-privada : RSA e curvas elípticas / Ana Carolina Sakurai Ferreira. -- Maringá, PR, 2019.
xi, 73 f.: il.

Orientadora: Profa. Dra. Claudete Matilde Webler Martins.
Coorientador: Prof. Dr. Rodrigo Martins.
Dissertação (Mestrado Profissional) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento de Matemática, Programa de Pós-Graduação em Matemática (PROFMAT) - Mestrado Profissional, 2019.

1. Criptografia RSA. 2. RSA (Sistema criptográfico). 3. Curvas elípticas. I. Martins, Claudete Matilde Webler, orient. II. Martins, Rodrigo, coorient. III. Universidade Estadual de Maringá. Centro de Ciências Exatas. Departamento de Matemática. Programa de Pós-Graduação em Matemática (PROFMAT) - Mestrado Profissional. IV. Título.

CDD 23.ed. 512.7

Márcia Regina Paiva de Brito - CRB-9/1267

CRIPTOGRAFIA DE CHAVE PÚBLICA-PRIVADA: RSA E CURVAS ELÍPTICAS

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Profa. Dra. Claudete Matilde Webler Martins
DMA/Universidade Estadual de Maringá (Orientadora)

Prof. Dr. Rodrigo Martins
DMA/Universidade Estadual de Maringá

Prof. Ms. Fabio Crivelli de Avila
Universidade de São Paulo – Avaré/SP

Prof. Dr. Francisco Nogueira Calmon Sobral
DMA/Universidade Estadual de Maringá

Aprovada em: 02 de agosto de 2019.
Local de defesa: Auditório do DMA, Bloco F67, campus da Universidade Estadual de Maringá.

Resumo

Neste trabalho estudamos dois criptossistemas de chave pública, o RSA e curvas elípticas a partir de uma adaptação do Problema do Logaritmo Discreto. São apresentados alguns embasamentos teóricos de aritmética, como estudo dos números primos e congruências. No final de cada criptossistema apresentamos um exemplo de uma mensagem/palavra criptografada utilizando o método estudado.

Palavras-chave: Criptografia, RSA, Curvas Elípticas.

Abstract

In this work we study two public key cryptosystems, the RSA and elliptic curves from an adaptation of the Discrete Logarithm Problem. Some theorical basis of arithmetic are presented, such as study of prime numbers and congruences. At the end of each cryptosystem we present an example of an encrypted message using the method studied.

Key-words: Cryptography, RSA, Elliptic Curves.

SUMÁRIO

LISTA DE FIGURAS

AGRADECIMENTOS

Agradeço, primeiramente, à Deus por me permitir vivenciar esta experiência e por ter me dado força para concluir este trabalho.

Agradeço ao meu esposo, Fernando, pela compreensão e paciência pelos momentos que tive que me ausentar para a elaboração deste trabalho.

Agradeço a minha família, minha mãe Alice, meu pai Adriano, e meus irmãos Jonas e João, que sempre acreditaram em mim e me apoiaram incondicionalmente.

Aos meus orientadores, Profa. Dra. Claudete Matilde Webler Martins e Prof. Dr. Rodrigo Martins, que foram fundamentais na realização e conclusão deste trabalho pela orientação, disponibilidade e pelos sábios conselhos.

A todos os professores que se dispuseram a ministrar aulas para nossa turma.

Agradeço aos meus colegas de mestrado Meibi Regina Oliveira da Silva, Priscila Cristina Andujar Moraes, Ana Paula e Fernando por todos os momentos de união, colaboração, pelas brincadeiras e conhecimentos compartilhados.

INTRODUÇÃO

Desde a antiguidade o envio e recebimento de informações sigilosas tem ocupado um papel de destaque na humanidade com um único objetivo: transmitir, com segurança, a mensagem de modo que somente o emissor e o receptor estejam a par da mesma. Tal procedimento de "modificar"a mensagem é denominado criptografia, procedente do grego cryptos que significa "secreto , oculto". Podemos perceber que a criptografia faz parte do nosso dia-a-dia, os códigos são usados naturalmente hoje por meio de celulares, bancos, internet, alarmes, barras de códigos e dentre outros.

Diante das múltiplas possibilidades de uso das criptografia e de sua fama atual este pode então, ser um tema de caráter motivador para se estudar matemática. Assim queríamos estudar alguma utilização disso que pudesse ser traduzida a uma linguagem mais palatável a todos os níveis de ensino para que isso servisse de fio condutor para despertar interesse em matemática. Desta forma nos debruçamos a entender o funcionamento da criptografia por tras do Bitcoin. Descobrimos que ele possui dois métodos de proteção: um protocolo de criptografia para dificultar a interceptação dos dados baseados em chaves públicas e privada e um protocolo de verificação de integridade de dados baseado em assinatura. Por um lado temos a

criptografia que serve para ocultar os dados transferidos e outro, a assinatura, que serve para verificar se os dados recebidos na transmissão não foram adulterados.

Entretanto, nenhum material que descreva os procedimentos, de forma completa, foi encontrado, muitos são os programas disponíveis para se repetir o processo usado no Bitcoin, chamado blockchain, mas quase nada aparece para descrever a teoria por tras da criptografia de blocos usada. Diante disso, percebemos que, por conta dos prazos, deveríamos restringir nosso objetivo inicial e aprender melhor a criptografia em chaves publicas e privadas, começando pela já bem estudada RSA e aplicando um pouco para a Criptografia em Curvas Elípticas utilizada no Bitcoin. Diante disso, nos limitamos assim ao estudo destes métodos sem adentrar na possibilidade de traduzir isso a um contexto escolar, que poderia ser um passo seguinte nesta pesquisa.

Diante disso, neste trabalho estudaremos dois tipos de criptografia, o método RSA e a criptografia envolvendo Curvas Elípticas (ECC).

No capítulo 1, abordaremos conceitos essenciais sobre números inteiros focando a atenção em números primos e congruências, destacando as principais proposições e teoremas que envolvem tais temas. O objetivo deste capítulo é dar o embasamento teórico para compreensão dos métodos RSA e Curvas Elípticas.

No capítulo 2, apresentaremos o problema do logaritmo discreto. Falaremos sobre como a dificuldade de resolução do logaritmo discreto auxilia na segurança do método de criptografia e apresentaremos dois algoritmos criptográficos: protocolo Diffie-Hellman e criptossistema ElGamal.

No capítulo 3, estudaremos e definiremos o funcionamento do método RSA e apresentaremos um exemplo de cifragem de mensagem com o uso do mesmo.

No capítulo 4, definiremos curvas elípticas a partir de uma modificação na equação de Weierstrass e a operação de soma sobre dois pontos de uma curva adaptando-a posteriormente para uma estrutura sobre um corpo $\mathbb{Z}_p$ seguido de um exemplo de

CAPÍTULO 1

NÚMEROS INTEIROS E DIVISÃO DOS INTEIROS

Neste capítulo estudaremos as propriedades dos números inteiros. Para tal é indispensável que o leitor tenha bem estabelecido a definição de números inteiros e o princípio da indução finita. Apresentaremos algumas proposições, teoremas e definições essenciais para estudos posteriores. O referencial teórico empregado neste capítulo é averiguado nas obras de [1], [2] e [3].

1.1 Divisão de Números Inteiros e Números primos

Nesta seção estudaremos propriedades relacionadas à números primos, divisão de números primos, divisibilidade e o método de fatoração de Fermat.

Observação: para não sobrecarregar o texto, não usaremos o ponto para indicar a multiplicação de dois números, a menos que isso possa causar confusão.

Definição 1.1. *Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Diz-se que b divide a ou b é divisor de a ou que a é múltiplo de b, se existe $c \in \mathbb{Z}$ tal que $a = bc$. Simbolicamente, podemos representar b divide a por $b|a$. Caso contrário, diz-se que b não divide a, e representa-se por $b \nmid a$.*

Proposição 1.2. *Sejam a,b e* $c \in \mathbb{Z}^*$. *Temos:*

(I) $1|a$, $a|a$ *e* $a|0$.

(II) $0|a$ *se, e somente se,* $a = 0$.

(III) Se $a|b$ *e* $b|c$, *então* $a|c$.

(IV) Se $a|b$ *e* $a|c$, *então* $a|(b \pm c)$.

(V) Se $a|b$, *então* $a|bc$.

(VI) Se $a|b$ *e* $a|(b \pm c)$, *então* $a|c$.

Demonstração:

(I) Decorre das igualdades $a = a.1$, $a = 1.a$ e $0 = 0.a$.

(II) Vamos supor que $0|a$; logo existe $c \in \mathbb{Z}$ tal que $a = c.0$ e concluímos que $a = 0$. Para a recíproca, basta observar que $0|0$, o que foi provado no item anterior.

(III) Temos, por hipótese, que $a|b$ e $b|c$, então existem $d, e \in \mathbb{Z}$ tais que

$$b = da \tag{1.1.1}$$

$$c = eb. \tag{1.1.2}$$

Substituindo (1.1.1) em (1.1.2) temos que $c = eb = (ed)a$, o que mostra que $a|c$.

(IV) Como $a|b$ e $a|c$, então, por definição, existem $f, g \in \mathbb{Z}$ tais que $b = af$ e $c = ag$. De modo que $b \pm c = (af) \pm (ag) = a(f \pm g)$. Logo $a|(b \pm c)$.

(V) Como $a|b$, por definição, existe $d \in \mathbb{Z}$ tal que $b = ad$, logo $bc = (ad)c = a(dc)$. Portanto $a|bc$.

(VI) Consideremos o caso $(b \pm c)$. Como $a|b$ e $a|(b \pm c)$, então, por definição, existem $d, f \in \mathbb{Z}$ tais que $b = da$ e $(b \pm c) = af$. Substituindo b na segunda igualdade temos: $b \pm c = (ad) \pm c = af$. Subtraindo ad de ambos os lados da igualdade temos: $c = af - ad = a(f - d)$, o que mostra que $a|c$.

□

1.1.1 Divisão Euclidiana

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

$$a = qb + r \text{ com } 0 \leq r < b$$

onde q é o quociente e r é o resto da divisão de a por b.

Demonstração: **Prova da existência.** Suponha, sem perda de generalidade, que $a \geq 0$ (pois no caso $a < 0$, multiplicamos por (-1)). Quando $a = 0$, temos que $q = r = 0$, quando $a = b$, temos que $q = 1$ e $r = 0$, quando $a \leq b$, temos que $q = 0$ e $r = a$. Logo vamos supor que $a > b$ e $a \geq 1$. Seja

$$\text{X} = \{n \in \mathbb{N}; n = bq + r, \text{ onde } 0 \leq r < b, q \in \mathbb{N}\}.$$

Assim,

(I) $1 \in X$, pois $1 = b.0 + 1$;

(II) Vamos supor por hipótese de indução que o resultado é válido para todo k, $1 \leq k \leq a - 1$, ou seja, $\{1, 2, 3, ..., a - 1\} \subseteq X$. Como $a > b > 0$, temos que $0 < a - b < a$. Pela hipótese de indução, existem $q_1, r \in \mathbb{Z}$, tais que

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

Fazendo $q = q_1 + 1$, obtém-se que

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

Unicidade. Vamos supor que existem $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tais que

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

e

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

Assim,

$$q_1 b + r_1 = a = q_2 b + r_2 \Leftrightarrow (q_1 - q_2)b = r_2 - r_1.$$

Temos também que

$$0 \leq r_2 < b \text{ e } -b < -r_1 \leq 0 \Rightarrow 0 \leq |r_2 - r_1| < b.$$

Logo,

$$|q_1 - q_2|b = |r_2 - r_1| < b \Rightarrow 0 \leqslant |q_1 - q_2| < 1.$$

Portanto, temos que $|q_1 - q_2| = 0$ e consequentemente $|r_2 - r_1| = 0$. Disto segue que $q_1 = q_2$ e $r_1 = r_2$

□

Exemplo 1.4. *Sejam $a = -75$ e $b = 9$. Determine a divisão de a por b.*

Solução:

$$-75 = (-9)9 + 6 \text{ onde } q = -9 \text{ e } r = 6.$$

1.2 Máximo Divisor Comum e Mínimo Múltiplo Comum

Definição 1.5. *Dados dois inteiros a e b, com $a \neq 0$ ou $b \neq 0$. Um número inteiro d será dito máximo divisor comum(mdc) de a e b se:*

(I) $d|a$ e $d|b$;

(II) Se c é divisor comum de a e b, então $c|d$.

Por (I) temos que d é divisor de a e b, e por (II) temos que d é o maior.

Exemplo 1.6. *O $mdc(12, 18) = 6$. Pois $6|12$ e $6|18$. Além disso, note que os divisores de 12 são: $1, 2, 3, 4, 6$ e 12 e os divisores de 18 são: $1, 2, 3, 6, 9$ e 18. Observe que 6 é divisível por todo divisor comum de 12 e 18.*

Teorema 1.7. *Dados dois inteiros a e $b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Então $d =$ mdc(a,b) existe. Além disso, existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$.*

Demonstração: Seja $X = \{ar + bs; r, s \in \mathbb{Z} \text{ e } ar + bs > 0\}$.

Então $X \neq \varnothing$ pois se $a \neq 0$, então $|a| = a.1 + b.0$ ou $|a| = a(-1) + b.0$. Assim, $|a| \in X$ e $X \subseteq \mathbb{N}$. Logo, X contém um menor elemento $d > 0$, ou seja, existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Agora vamos mostrar que $d =$ mdc(a,b). Tomemos $q, r \in \mathbb{Z}$ tais que $a = qd + r$, onde $0 \leq r < d$. Então,

$$r = a - qd = a(1 - qx) + b(-qy) \Rightarrow r = 0,$$

pois se $r > 0$, então $r \in X$, o que é uma contradição. Logo, $a = qd$, ou seja, $d|a$. Analogamente, mostra-se que $d|b$. Assim, se $c|a$ e $c|b$ então $c|(ax + by)$, ou seja, $c|d$.

□

Dados $a, b \in \mathbb{Z}^*$, dizemos que a e b são relativamente primos, quando mdc(a,b) = 1.

Teorema 1.8. *Sejam $a, b \in \mathbb{Z}^*$. Então a e b são relativamente primos se, e somente se, existem $x, y \in \mathbb{Z}$ tais que*

$$ax + by = 1$$

Demonstração: Suponha que existam $x, y \in \mathbb{Z}$ tais que $ax+by = 1$ e $d = \text{mdc(a,b)}$, então $d \mid 1$ e logo $d = 1$. A recíproca é imediata pelo Teorema 1.7.

□

Lema 1.9. *Sejam $a, b, c \in \mathbb{Z}^*$. Então mdc(ac,bc) =| c | mdc(a,b).*

A ocorrência $c \mid ab$ não garante que $c \mid a$ ou $c \mid b$. Veja:

$$4 \mid 2.10 \text{ } mas \text{ } 4 \nmid 2 \text{ } e \text{ } 4 \nmid 10$$

Demonstração: Sejam $a, b, c \in \mathbb{Z}^*$. Se $c|ab$ e mdc(a,c) = 1, então $c|b$.

Se mdc(a,c) = 1, então existem $x, y \in \mathbb{Z}$ tais que $ax + cy = 1$. Assim,

$$abx + bcy = b$$

Como $c|ab$ e $c|c$, tem-se que $c|(abx + bcy)$, isto é $c|b$.

□

Lema 1.10. *Sejam $a, b, r \in \mathbb{Z}^*$. Se $a = qb + r$, onde $0 \leq r < b$, então mdc(a,b) = mdc(b,r).*

Para determinar o máximo divisor comum entre dois inteiros a e b, é utilizado o Algoritmo de Euclides (Veja Tabela 1.1).

	q_1	q_2	q_3	...	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-1}	r_n
r_1	r_2	r_3	...	r_n	0	

Tabela 1.1: Algoritmo de Euclides

Supondo que $a \geq b > 0$, pois mdc(a,b) =mdc($\mid a \mid, \mid b \mid$).

Então existem $q_1, r_1 \in \mathbb{Z}$ tais que $a = q_1 b + r_1$, onde $0 \leq r_1 < b$.

Se $r_1 = 0$, então $b|a$ e mdc(a,b) $= b$. Se $r_1 \neq 0$, então existem $q_2, r_2 \in \mathbb{Z}$ tais que $b = q_2 r_1 + r_2$ onde $0 \leq r_2 < r_1$.

Se $r_2 = 0$, então $r_1|b$ e mdc(a,b) = mdc(b,r_1) $= r_1$. Se $r_2 \neq 0$, então existem $q_3, r_3 \in \mathbb{Z}$ tais que $r_1 = q_3 r_2 + r_3$, onde $0 \leq r_3 < r_2$ e assim sucessivamente até que algum resto seja nulo, isto é, $r_{n+1} = 0$. Obtendo assim as seguintes relações:

$$\begin{array}{ccccc}
a & = & q_1 b + r_1 & \text{onde} & 0 \leq r_1 < b; \\
b & = & q_2 r_1 + r_2 & \text{onde} & 0 \leq r_2 < r_1; \\
r_1 & = & q_3 r_2 + r_3 & \text{onde} & 0 \leq r_3 < r_2; \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
r_{n-3} & = & q_{n-1} r_{n-2} + r_{n-1} & \text{onde} & 0 \leq r_{n-1} < r_{n-2}; \\
r_{n-2} & = & q_n r_{n-1} + r_n & \text{onde} & 0 \leq r_n < r_{n-1}; \\
r_{n-1} & = & q_{n+1} r_{n+1}. & &
\end{array}$$

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

Exemplo 1.11. *Determine o máximo divisor comum entre 372 e 162.*

Considere o Algoritmo de Euclides,

	2	*3*	*2*	*1*	*2*
372	*162*	*48*	*18*	*12*	*6*
48	*18*	*12*	*6*	*0*	

Assim, mdc(372,162) = 6.

Observação 1.12. *O Algoritmo de Euclides também é utilizado para representar o mdc(a,b) na forma $ax + by$. Observe que da penúltima e antepenúltima equações tem-se*

$$r_n = r_{n-2} + (-q_n) r_{n-1}; \tag{1.2.1}$$

$$r_{n-1} = r_{n-3} + (-q_{n-1})r_{n-2}. \tag{1.2.2}$$

Substituindo o resto r_{n-1} *de (1.2.1) em (1.2.2), obtém-se*

$$r_n = (-q_n)r_{n-3} + (1 + q_n q_{n-1})r_{n-2}$$

Com esse procedimento são eliminados sucessivamente os restos

$$r_{n-1}, r_{n-2}, \ldots, r_2, r_1$$

e r_n *é determinado em termos de* a *e* b*, isto é, encontra-se* $x, y \in \mathbb{Z}$ *tais que*

$$mdc(a,b) = ax + by.$$

Definição 1.13. *Diremos que um número inteiro* $m \geq 0$ *é um mínimo múltiplo comum (mmc) dos números inteiros* a *e* b*, se possuir as seguintes propriedades:*

(I) m *é um múltiplo comum de* a *e* b*;*

(II) se c *é um múltiplo comum de* a *e* b*, então* $m|c$*.*

Exemplo 1.14. *Temos que* $mmc(2,3) = 6$*, pois* 6 *é múltiplo comum de* 2 *e* 3 *e além disso* 12 *é um múltiplo comum de* 2 *e* 3 *e* $6|12$*.*

1.3 Números Primos

Definição 1.15. *Um número inteiro* $p > 2$ *é dito primo se seus únicos divisores positivos são* 1 *e* p*,caso contrário* p *é considerado número composto.*

Exemplo 1.16. *O número* 5 *é primo, pois tem como divisores apenas o* 1 *e o* 5 *enquanto que o número* 4 *é composto pois seus divisores são* $1, 2$ *e* 4*.*

Proposição 1.17. *Sejam* a*,*b *e* $p \in \mathbb{Z}$ *com* p *primo. Se* $p|ab$ *então* $p|a$ *ou* $p|b$*.*

Demonstração: Vamos supor que $p \nmid a$. Então os divisores comuns de p e a são apenas 1 e -1. Logo, o $mdc(a, p) = 1$. Assim existem x e $y \in \mathbb{Z}$ tais que

$$1 = ax + py.$$

Multiplicando ambos os membros da igualdade por b, temos $b = (ab)x + p(by)$. Como $p|(ab)$ existe um $k \in \mathbb{Z}$ tal que $ab = kp$. Sabemos que $p|p$, então

$$b = (kp)x + p(by) = p(kx + by)$$

Logo, $p|b$.

□

Corolário 1.18. *Se p é um primo tal que $p|p_1 \cdots p_n$, então $p|p_i$ para algum $i = 1, \cdots, n$.*

Demonstração: Vamos utilizar o processo da indução finita. A afirmação é verdadeira para $n = 1$ e para $n = 2$(consequência da Proposição 1.17). Supondo, então $n > 2$ e que, se p divide um produto com $n - 1$ fatores, então p divide pelo menos um dos fatores. Note que, se $p|p_1 \cdots p_n$, então $p|p_n$ ou $p|p_1 \cdots p_{n-1}$, logo a hipótese de indução garante que $p|p_k$, com $1 < k < n-1$. Ambos os casos, p divide um dos inteiros $p_1, p_2, \cdots, p_n$. □

Corolário 1.19. *Se $p, p_1 \cdots p_n$ são números primos e se $p|p_1 \cdots p_n$, então $p = p_i$ para algum $i = 1, \cdots, n$.*

Demonstração: Note que existe um índice k, onde $1 < k < n$, tal que $p|p_k$, como os únicos divisores positivos de p_k são 1 e p_k, pois p_k é primo, segue-se que $p = 1$ ou $p = p_k$. Mas, $p > 1$, pois p é primo. Logo, $p = p_k$. □

Teorema 1.20. *(Teorema Fundamental da Aritmética) Todo inteiro maior do que 1*

é primo ou pode ser representado de maneira única (a menos da ordem dos fatores) como um produto de fatores primos.

Demonstração: Vamos utilizar o processo da indução finita. Se $n = 2$, o resultado é óbvio pois 2 é primo. Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, não há o que demonstrar. Se n for composto, existem números inteiros positivos n_1 e n_2 tais que $n = n_1.n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem primos $p_1, p_2, \cdots, p_r$ e $\overline{p}_1\overline{p}_2 \cdots \overline{p}_s$, tais que $n_1 = p_1p_2 \cdots p_r$ e $n_2 = \overline{p}_1\overline{p}_2 \cdots \overline{p}_s$. Logo,

$$n = p_1p_2 \cdots p_r\overline{p}_1\overline{p}_2 \cdots \overline{p}_s.$$

Vamos provar a unicidade da representação. Suponha, agora, que $n = p_1p_2 \cdots p_r = q_1q_2 \cdots q_s$, onde os p_i e os q_j são números primos. Como $p_1|q_1q_2 \cdots q_s$, temos que $p_1 = q_j$ para algum $j \leq s$, que, ao reordenarmos os fatores $q_1, q_2, \cdots, q_s$ podemos chamar de q_1. Logo,

$$p_2 \cdots p_r = q_2 \cdots q_s$$

Como $p_2 \cdots p_r < n$, a hipótese de indução implica em $r = s$ e os p_i e q_j são iguais aos pares, o que mostra a unicidade da fatoração de n. □

Teorema 1.21. *Existem infinitos números primos.*

Demonstração: Suponhamos, por contradição, que a quantidade de números primos seja finita e seja $p = \{p_1, p_2, \cdots, p_n\}$ o conjunto de todos os primos. Seja $R = p_1p_2p_3 \cdots p_n + 1$; note que R é maior que qualquer $p_i \in P$ e nenhum elemento de P é fator de R. Pelo Teorema Fundamental da Aritmética, ou R é primo ou possui algum fator primo, isto implica na existência de um primo que não pertence a P. Portanto P não pode ser um conjunto finito. □

1.4 Descobrindo se o número é primo

Sabemos que um número primo p possui apenas dois divisores: 1 e ele mesmo. Para verificar se um dado número n é primo ou não devemos encontrar divisores primos de n efetuando as divisões até n. A proposição seguinte nos garante que não precisamos efetuar todas as divisões, vejamos:

Proposição 1.22. *Se p é o menor fator primo de n então $p \leq \sqrt{n}$.*

Demonstração: Denotaremos por $D(n)$ o conjunto dos divisores positivos de n diferentes de 1 ou n. Como n não é primo, temos que $D(n) \neq \varnothing$. Seja $p \in D(n)$ tal que, para todo $q \in D(n)$ tem-se $p \leq q$. Supondo que $p > \sqrt{n}$ e que $n = p.q$. Temos $q \geq p > \sqrt{n}$. Assim $n = (\sqrt{n})^2 < p.q = n$, o que é um absurdo. Logo, $p \leq \sqrt{n}$. $\square$

Exemplo 1.23. *Para determinar se o número 179 é primo basta tentarmos dividi-lo pelos primos menores ou igual a 13 que é, aproximadamente, sua raiz quadrada:*

$179 = 89.2 + 1$
$179 = 59.3 + 2$
$179 = 35.5 + 4$
$179 = 25.7 + 4$
$179 = 16.11 + 3$
$179 = 13.13 + 10$

Logo, 179 é primo.

1.5 Congruências

Nesta seção, estudaremos a Aritmética dos Restos da Divisão Euclidiana por um número fixo. Alguns métodos de criptografia, principalmente o RSA são baseados em cálculos que envolvem congruências. Sendo assim, veremos algumas definições e proposições sobre o mesmo.

Definição 1.24. *Seja m um número natural. Dizemos que dois números a e b são congruentes módulo m se os restos de sua divisão euclidiana por m forem iguais. Escreve-se:*

$$a \equiv b \ mod \ m$$

Exemplo 1.25. $41 \equiv 14 \ mod \ 3$ *, pois os restos da divisão de* 41 *e* 14 *por* 3 *são iguais a* 2*.*

Proposição 1.26. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$. Temos que $a \equiv b \ mod \ m$ se, e somente se, $m|b - a$.*

Demonstração: Podemos escrever as divisões euclidianas de a e b por m como: $a = m.q + r$, com $0 \leq r < m$ e $b = m.q' + r'$, com $0 \leq r' < m$, respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r).$$

Assim, $a \equiv b \bmod m$ se, e somente se, $r = r'$, e pela igualdade acima, é equivalente a dizer que $m|b - a$, já que $r - r' = 0$. □

Proposição 1.27. *Seja $m \in \mathbb{N}$. Para quaisquer $a, b, c \in \mathbb{Z}$, temos que:*

(I) $a \equiv a \ mod \ m$*,*

(II) Se $a \equiv b \ mod \ m$*, então* $b \equiv a \ mod \ m$*,*

(III) Se $a \equiv b \ mod \ m$ *e* $b \equiv c \ mod \ m$*, então* $a \equiv c \ mod \ m$*.*

Demonstração:

(I) $a \equiv a \bmod m$ pois $m|(a - a) = 0$;

(II) Se $a \equiv b \bmod m$, então temos que $m|(b - a)$ logo, existe um inteiro x tal que $b - a = x.m$, então $-xm = -(b - a) = (a - b)$. Assim podemos deduzir que $m|(a - b)$, ou seja, $b \equiv a \bmod m$.

(III) Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $m|(b-a)$ e $m|(c-b)$, então

$$m|[(b-a)+(c-b)],$$

assim $m|(-a+c)$. Portanto $a \equiv c \bmod m$.

□

Proposição 1.28. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.*

(I) Se $a \equiv b$ mod m e $c \equiv d$ mod m, então $a + c \equiv b + d$ mod m;

(II) Se $a \equiv b$ mod m e $c \equiv d$ mod m, então $ac \equiv bd$ mod m.

Demonstração:

(I) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $m|(b-a)$ e $m|(d-c)$ logo, $m|[(b-a)+(d-c)]$ o que equivale a $m|(b-a+d-c)$, ou seja, $m|(b+d-a-c)$, ou $m|[(b+d)-(a+c)]$. Logo $a + c \equiv b + d \bmod m$.

(II) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $m|(b-a)$ e $m|(d-c)$. Fazendo $bd - ac = d(b-a) + a(d-c)$, como $m|[d(b-a)+a(d-c)]$, concluímos que $m|(bd-ac)$, portanto $ac \equiv bd \bmod m$.

□

Corolário 1.29. *Para todo $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b$ mod m, então tem-se que $a^n \equiv b^n$ mod m.*

Demonstração: Vamos utilizar o princípio da indução finita. Para $n = 1$ a sentença é verdadeira. Suponhamos que $a^n \equiv b^n \bmod m$ como verdadeira, então pela Proposição 1.28 temos que $a.a^n \equiv b.b^n \bmod m \Rightarrow a^{n+1} \equiv b^{n+1} \bmod m$, o que mostra que a propriedade é verdadeira. □

Exemplo 1.30. *Mostre que* $45|(13^{3n} + 17^{3n})$*, para todo número natural ímpar* n*.*

Note que, usando a Proposição 1.28 e o Corolário 1.29,

$13^3 = 13^2.13 \equiv 34.13 = 442 \equiv 37 \equiv -8 \ mod\ 45$*, (Aqui, como o resto é* 37*, sabemos que faltam* 8 *unidades para chegarmos em* 45*, por isso representamos por* -8*).*

Logo,

$$13^3 \equiv -8 \ mod\ 45.$$

Como n *é ímpar, temos que*

$$13^{3n} \equiv -8^n \ mod\ 45. \tag{1.5.1}$$

Por outro lado, temos que

$$17^3 = 17^2.17 \equiv 19.17 = 323 \equiv 8 \ mod\ 45.$$

Logo,

$$17^{3n} \equiv 8^n \ mod\ 45. \tag{1.5.2}$$

*Por (*1.5.1*) e (*1.5.2*) temos que*

$$13^{3n} + 17^{3n} \equiv -8^n + 8^n \equiv 0 \ mod\ 45.$$

Portanto $45|13^{3n} + 17^{3n}$*.*

Proposição 1.31. *Sejam* $a, b, c, m \in \mathbb{Z}$*, com* $m > 1$*. Tem-se que*

$$a + c \equiv b + c \ mod\ m \Leftrightarrow a \equiv b \ mod\ m$$

Demonstração: Se $a \equiv b \bmod m$, então temos que $a + c \equiv b + c \bmod m$, pois $c \equiv c \bmod m$. Agora, se $a+c \equiv b+c \bmod m$, então $m|[b+c-(a+c)]$, o que implica que $m|(b-a)$, logo $a \equiv b \bmod m$. □

Proposição 1.32. *Sejam $a, b, c, m \in \mathbb{Z}$, com $c \neq 0$ e $m > 1$. Temos que $ac \equiv bc \ mod \ m \Leftrightarrow a \equiv b \ mod \ \frac{m}{mdc(c,m)}$.*

Demonstração: Como $\frac{m}{\text{mdc}(c,m)}$ e $\frac{c}{\text{mdc}(c,m)}$ são coprimos, temos que

$$ac \equiv bc \bmod m \Leftrightarrow m|(b-a)c$$

dividindo ambos os termos por $\text{mdc}(c,m)$ temos:

$$\frac{m}{\text{mdc}(c,m)} \mid (b-a)\frac{c}{\text{mdc}(c,m)}$$

que é equivalente a

$$\frac{m}{\text{mdc}(c,m)} \mid (b-a)$$

ou seja

$$a \equiv b \bmod \frac{m}{\text{mdc}(c,m)}.$$

□

Da proposição acima temos que:

Dados $a, b, c, m \in \mathbb{Z}$ com $c \neq 0$, $m > 1$ e $mdc(c,m) = 1$, então $ac \equiv bc \bmod m$ se, e somente se, $a \equiv b \bmod m$ pela Proposição 1.32. Sendo k denominado o inverso de c módulo m.

Proposição 1.33. *Se existir um fator primo comum entre a e m, então a não admite inverso módulo m.*

Demonstração: Digamos que m e a são inteiros positivos tais que $1 < a < m$. Existe um inteiro p tal que $1 < p$, $p|a$ e $p|m$. Vamos supor que existe um $b \in \mathbb{Z}$ tal que $ab \equiv 1 \bmod m$. Logo existe um q inteiro tal que $ab - 1 = qm$ ou $1 = ab - qm$. Por hipótese temos que $p|a$, então $p|ab$ e $p|m$, então $p|qm$. Assim $p|(qm - ab)$, mas isso implicaria em $p|1$, o que é um absurdo pois $1 < p$, portanto, não existe tal b.

□

1.5.1 Teorema de Fermat

Este teorema é um resultado de grande valia para a divisibilidade na Teoria dos Números. Muito utilizado para determinar restos de divisões de potências elevadas. No final desta sessão apresentaremos alguns exemplos clássicos desta aplicação.

Teorema 1.34. *Se p é primo então:*

$$a^p \equiv a \ mod \ p,$$

para todo $a \in \mathbb{N}$.

Para a demonstração do teorema acima utilizaremos o seguinte lema.

Lema 1.35. *Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.*

A demonstração deste lema pode ser encontrada em [4].

Agora vamos voltar a demonstração do Teorema 1.34, também conhecido como Pequeno Teorema de Fermat (P.T.F).

Demonstração: Para $p = 2$ temos que o resultado é imediato pois $a^2 - a = a(a-1)$, se a for par temos que $2|a(a-1)$. Agora se a for ímpar , $a-1$ será par e $2|a(a-1)$. Seja p primo, $p > 2$. Faremos a prova usando o processo de Indução Finita sobre a. Para $a = 0$ temos

$$0^p - 0 = 0 \text{ e } p|0.$$

Vamos supor que vale para a e vamos mostrar que implica em $p|a+1$, ou seja, $p|[(a+1)^p - (a+1)]$.

Note que

$$(a+1)^p - (a+1) = \binom{p}{0}.a^p.1^0 + \binom{p}{1}a^{p-1}.1^1 + \cdots + \binom{p}{p-1}.a^1 + 1 - a - 1$$

$$= a^p + \binom{p}{1}.a^{p-1} + \cdots + \binom{p}{p-1}.a - a$$
$$= a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}.a.$$

Pelo lema anterior temos que $\binom{p}{1}.a^{p-1} + \cdots + \binom{p}{p-1}.a$ é divisível por p e por hipótese $a^p - a$ é divisível por p, logo $a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}.a$ é divisível por p.

□

Teorema 1.36. *Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$, ou seja, a^{p-1} mod p.*

Demonstração: Observe que $a(a^{p-1} - 1) = a^p - a$, assim, pelo Pequeno Teorema de Fermat, temos que $p|a(a^{p-1} - 1)$ e por hipótese p não divide a, e $mdc(p, a) = 1$. Portanto $p|a^{p-1} - 1$. □

O Teorema 1.36 é um caso particular do Pequeno Teorema de Fermat.

Exemplo 1.37. *Determine o resto da divisão de 5^{234} por 11.*

Note que 11 é primo e $mdc(11, 5) = 1$, observe que $5^{10} \equiv 1$ mod 11 pelo Pequeno Teorema de Fermat, temos:

$$5^{234} \equiv 5^{10.23+4} \equiv (5^{10})^{23}.5^4 \equiv 1^{23}.5^4 \equiv 5^4 \equiv 625 \equiv 9 \text{ mod } 11.$$

Exemplo 1.38. *Encontre o resto da divisão de $2^{1000000}$ por 17.*

Note que 17 é primo e não divide 2, então pelo Pequeno Teorema de Fermat

$$2^{16} \equiv 1 \text{ mod } 17 \text{ mas } 1000000 = (62500).(16).$$

Logo,

$$2^{1000000} = (2^{16})^{62500} \equiv 1^{62500} \equiv 1 \text{ mod } 17$$

Assim, temos que o resto da divisão de $2^{1000000}$ *por* 17 *é* 1.

Exemplo 1.39. *Mostre que* $42|(a^7 - a)$ *para todo número natural* a.

Temos que $42 = 2.3.7$*, todos números primos, vamos provar que cada um deles divide* $(a^7 - a)$.

(I) Temos que $a^7 \equiv a \ mod\ 7$*, pela aplicação do Pequeno Teorema de Fermat (caso* $a \neq 7$*). Para* $a = 7$ *temos que* $a^7 - a = 7(7^6 - 1)$ *que é múltiplo de* 7 *também. Logo,* $7|(a^7 - a)$*, para todo* a *natural.*

(II) Temos que $3|(a^7 - a)$ *pois,*

$$a^7 - a = a(a^6 - 1) = a[(a^2)^3 - 1] = a[(a^2 - 1)(1 + a^2 + a^4)] = (a^3 - a)(1 + a^2 + a^4)$$

Pelo Pequeno Teorema de Fermat temos que $a^3 \equiv a \ mod\ 3$ *então* $3|(a^3 - a)$ *logo,* $3|(a^7 - a)$.

(III) Temos que $2|(a^7 - a)$ *pois,*

$$a^7 - a = a(a^6 - 1) = a[(a^2 - 1)(1 + a^2 + a^4)] = a[(a - 1)(a + 1)(1 + a^2 + a^4)]$$

$$= (a^2 - a)(a + 1)(1 + a^2 + a^4)$$

Pelo Pequeno Teorema de Fermat temos que $a^2 \equiv a \ mod\ 2$ *logo,* $2|(a^7 - a)$

Dos itens acima concluímos que $42|(a^7 - a)$.

1.5.2 Teorema de Euler

Antes de mencionar o Teorema de Euler, veremos algumas definições, proposições e lemas que contribuirão na demonstração do mesmo.

Definição 1.40. *Chama-se função aritmética, toda função f definida no conjunto $\mathbb{N}$ dos naturais e com valores no conjunto $\mathbb{Z}$ dos inteiros, isto é, toda função f de $\mathbb{N}$ em $\mathbb{Z}$ ($f : \mathbb{N} \longrightarrow \mathbb{Z}$).*

Definição 1.41. *Chama-se Função Totiente a função aritmética $\phi(n)$ que denota a quantidade de inteiros $k \in \{1, 2, 3, \cdots, n\}$, tais que $mdc(k, n) = 1$.*

Proposição 1.42. *Seja ϕ a Função Totiente.*

(I) Se p é primo, então $\phi(p) = p - 1$.

(II) Sejam m e n inteiros positivos, ambos maiores que 1, e $mdc(m, n) = 1$ então $\phi(m.n) = \phi(m).\phi(n)$.

Demonstração:

(I) Tome o conjunto $Q = \{1, 2, 3, \cdots, p-1\}$ dos números inteiros menores que p. Como p é primo nenhum elemento de Q é fator de p, assim para todo $k \in Q$, $mdc(k, p) = 1$. Como há p - 1 elementos Q, temos o desejado.

(II) Vamos supor que m e n são ambos primos para utilizarmos a propriedade (I). Temos que $\phi(m) = m - 1$ e $\phi(n) = n - 1$ e o produto $\phi(m).\phi(n) = mn-m-n+1$. O conjunto $P = \{1, 2, 3, m, n, \cdots, mn\}$ possui $m-1$ elementos $k_1, k_2, \cdots, k_{m-1}$ tais que $mdc(k_i, mn) = n$ e $n-1$ elementos $l_1, l_2, \cdots, l_{m-1}$ tais que $mdc(l_i, mn) = m$ e o próprio mn. Para os demais elementos dos $p_i \in P$, temos: $mdc(p_i, mn) = 1$ então a quantidade de elementos p_i de P é dada por $mn - (m - 1) - (n - 1) - 1$ logo $\phi(mn) = mn - m - n + 1$ o que confirma a propriedade.

□

A propriedade (II) nos garante que se n é o produto de dois números primos p e q temos que $\phi(n) = (p - 1)(q - 1)$.

Lema 1.43. *Sejam a e $n > 1$ inteiros tais que o $mdc(a, n) = 1$. Se $a_1, a_2, \cdots, a_k$ são inteiros positivos menores que n e cada um deles coprimo com n, então cada um dos inteiros $a.a_1, a.a_2, \cdots, a.a_k$ é congruente módulo n a um dos inteiros $a_1, a_2, \cdots, a_k$ (não necessariamente nesta ordem em que aparecem).*

A base teórica utilizada para a demonstração deste lema é o mesmo utilizado na prova do Pequeno Teorema de Fermat.

Teorema 1.44. *(Teorema de Euler) Se n é um inteiro positivo e se $mdc(a, n) = 1$, então:*

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

Demonstração: Para $n = 1$ a proposição é verdadeira, pois $a^{\phi(1)} \equiv 1 \bmod 1$. Suponhamos, $n > 1$, e sejam $a_1, a_2, \cdots, a_{\phi(n)}$ os inteiros positivos menores que n e relativamente primos a n. Como o $mdc(a, n) = 1$, então, pelo Lema 1.43 os inteiros $a.a_1, a.a_2, \cdots, .a.a_{\phi(n)}$ são congruentes módulo n aos inteiros $a_1, a_2, \cdots, a_{\phi(n)}$ em uma certa ordem:

$$a.a_1 \equiv a_{1'} \bmod n, a.a_2 \equiv a_{2'} \bmod n, \cdots, a.a_{\phi(n)} \equiv \phi(n)' \bmod n,$$

onde $a_{1'}, a_{2'}, \cdots, a_{\phi(n)'}$ denotam os inteiros $a_1, a_2, \cdots, a_{\phi(n)}$ em uma certa ordem. Multiplicando ordenadamente todas essas $\phi(n)$ congruências, obtemos:

$$(a.a_1).(a.a_2) \cdots (a.a_{\phi(n)}) \equiv a_{1'}.a_{2'} \cdots a_{\phi(n)'} \bmod n,$$

ou seja,

$$a^{\phi(n)}.(a_1.a_2 \cdots a_{\phi(n)}) \equiv a_1.a_2 \cdots a_{\phi(n)} \bmod n.$$

Sendo cada um dos inteiros $a_1, a_2 \cdots a_{\phi(n)}$ coprimo com n, de modo que podem ser sucessivamente cancelados, o que dá a congruência de Euler:

$$a^{\phi(n)} \equiv 1 \bmod n.$$

□

Observação: Se p é um número primo, $\phi(p) = p - 1$, e se $mdc(a, p) = 1$, então $a^{\phi(p)} \equiv a^{p-1} \bmod p \equiv 1 \bmod p$, que é uma generalização do Teorema de Fermat.

Corolário 1.45. *Se $m > 1$, $k \geqslant 0$, $n \geqslant 0$, e a um inteiro qualquer são tais que, $mdc(a, m) = 1$ e $k \equiv n \ mod \ (\phi(m))$ então, $a^k \equiv a^n \ mod \ m$.*

Demonstração: Consideremos o caso em que $k > n$. Como $k \equiv n \bmod (\phi(m))$ existe $q \geqslant 1$ tal que $k - n = q.\phi(m)$ e, portanto,

$$a^k = a^{k-n}.a^n = a^{q.\phi(m)}.a^n = (a^{\phi(m)})^q.a^n \equiv a^n \bmod m.$$

□

O Teorema de Euler tem uma participação fundamental na resoluções de congruências lineares. Dado $mdc(a, m) = 1$, a congruência linear $a.x \equiv b \bmod m$, admite uma única solução módulo m. Com efeito, da expressão temos

$$a.x \equiv b \bmod m$$

obtemos

$$a.x \equiv b.a^{\phi(m)} \bmod m.$$

Como $mdc(a, m) = 1$, podemos cancelar o fator comum a, que resulta em

$$x \equiv b.a^{\phi(m)-1} \bmod m.$$

Exemplo 1.46. *Determine x na congruência $2x \equiv 9$ mod 25.*

Como $mdc(2, 25) = 1$, temos que

$$x \equiv 9.2^{\phi(25)-1} \equiv 9.2^{20-1} \equiv 9.2^{19} \equiv 9.524288 \equiv 4718592 \equiv 17 \ mod \ 25$$

Note que 17 *é o valor procurado, pois* $2.17 = 34 \equiv 9$ *mod* 25.

Podemos perceber que, $a.x \equiv 1 \bmod n$ implica em $x \equiv a^{\phi(n)-1} \bmod n$ o que nos leva a concluir que $a^{\phi(n)-1}$ é o inverso multiplicativo de a módulo n se $mdc(a, n) = 1$.

Exemplo 1.47. *Determine o inverso multiplicativo de* 5 *módulo* 11.

Note que $mdc(5, 11) = 1$, *então, pelo Teorema de Euler temos* $x = 5^{\phi(11)-1} \equiv 5^{10-1} \equiv 5^9 \equiv 1953125 \equiv 9$ *mod* 11, *assim,* $x = 9$ *é o menor inverso multiplicativo de* 5 *módulo* 11.

1.5.3 Sistemas de Congruências Lineares

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

Esse problema foi proposto pelo matemático Sun-Tsu e a resposta dada por ele para este problema foi 23.

A resolução desse problema é baseada em procurar as soluções do seguinte sistema de congruências:

$$X \equiv 2 \bmod 3$$
$$X \equiv 3 \bmod 5$$
$$X \equiv 2 \bmod 7.$$

Uma maneira de resolução para este sistema será mostrada logo após o seguinte teorema:

Teorema 1.48. *Teorema Chinês do Resto (restrito a duas congruências com módulos primos entre si). Sejam* m *e* n *inteiros positivos primos entre si. Se* a *e* b *são inteiros quaisquer, então o sistema*

$$\begin{cases} x \equiv a \ mod \ m \\ x \equiv b \ mod \ n \end{cases}$$

sempre tem solução e qualquer uma de suas soluções pode ser escrita na forma $a+m.(m'.(b-a)+n.t)$*; onde* t *é um inteiro qualquer e* m' *é o inverso de* m *módulo* n*.*

Demonstração: Considere o sistema: $\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}$ onde m e n são inteiros positivos distintos e digamos que o número inteiro x_0 é uma solução desta congruência. Isto significa que x_0 satisfaz a ambas as congruências:

$$\begin{cases} x_0 \equiv a \bmod m \\ x_0 \equiv b \bmod n. \end{cases}$$

Como os módulos são diferentes, só podemos combinar as duas congruências se convertermos uma delas em uma igualdade de inteiros. Fazendo isto com a primeira equação, verificamos que

$$x_0 = a + m.k$$

onde k é um inteiro qualquer, de forma que podemos concluir que

$$a + mk \equiv b \bmod n,$$

ou ainda,

$$mk \equiv (b-a) \bmod n.$$

Supondo que m e n sejam primos entre si, temos que m é inversível módulo n. Digamos que m' é o inverso de m módulo n ou $m.m' \equiv 1 \bmod n$. Multiplicando $m.k \equiv (b-a) \bmod n$ por m', obtemos

$$k \equiv m'(b-a) \bmod n$$

ou seja,

$$k \equiv m'(b-a) + nt$$

para algum inteiro t. Substituindo esta expressão para k em $x_0 = a + m.k$, vemos que

$$x_0 = a + m(m'(b-a) + nt)$$

Logo, x_0 é uma solução do sistema. □

Exemplo 1.49. *Determinar o menor número inteiro que dividido por* 3 *tem resto* 1 *e dividido por* 5 *tem resto* 2.

Devemos determinar um valor x *que satisfaça o sistema de congruências:*

$$\begin{cases} x \equiv 1 \ mod\ 3 \\ x \equiv 2 \ mod\ 5. \end{cases}$$

Chamando m' *o inverso de* 3 *mod* 5*, temos que* $m' = 2$*, visto que* $3.2 = 6 \equiv 1 \ mod\ 5$*. Pela fórmula do Teorema Chines dos Restos, temos que* x_0 *é uma solução:*

$$x_0 = 1 + 3(2.(2-1) + 5t) = 1 + 6 + 15t = 7 + 15t$$

Logo $x = 7$ *é a menor solução positiva para o problema dado.*

Esse tipo de problema não fica restrito somente a sistemas de duas congruências. Estudaremos um caso particular de sistema por substituição utilizando os Teoremas de Fermat e Euler.

Exemplo 1.50. *Encontre o menor inteiro positivo* x *que satisfaz o seguinte sistema de congruências:*

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

note que $mdc(3.5) = 1$*,* $mdc(3.7) = 1$ *e* $mdc(5.7) = 1$*, da primeira equação temos que existe um inteiro* y *tal que:* $X = 3y + 1$*. Substituindo na segunda congruência, temos:* $3y + 1 \equiv 2 \ mod\ 5$*, que implica em* $3y \equiv 1 \ mod\ 5$*, onde* $y = 3^{\phi(5)-1} \equiv 3^3 \equiv 27 \equiv 2 \ mod\ 5$*, que significa que existe um* k*, inteiro, tal que* $y = 5k + 2$*.*

Agora temos $X = 3(5k + 2) + 1$ *onde* $X = 15k + 7$. *Substituindo na terceira congruência, temos:* $15k + 7 \equiv 3 \ mod\ 7$, *que implica em* $15k \equiv -4 \ mod\ 7$, *sendo* $k \equiv -4 \equiv 3 \ mod\ 7$ *que significa que existe um* U, *inteiro tal que* $k = 7U + 3$. *Finalmente* $X = 15.(7U + 3) + 7$ *implica que* $X = 105U + 52$. *Então* $X = 52$ *é a menor solução positiva para este sistema de congruências.*

CAPÍTULO 2

PROBLEMA DO LOGARITMO DISCRETO

Neste capítulo falaremos sobre o Problema do Logaritmo Discreto. O referencial teórico empregado neste capítulo é averiguado nas obras de [5], [6],[7] e [8].

A dificuldade de resolver o Problema do Logaritmo Discreto é a base de alguns sistemas de criptografia de chave pública, entre eles a criptografia com curvas elípticas.

Seja (G, x) um grupo multiplicativo e $\alpha, \beta \in G$. O Problema do Logaritmo Discreto consiste em encontrar o valor de $x \in \mathbb{Z}$ tal que

$$\alpha^x = \beta,$$

onde o inteiro x indicado por $\log_\alpha \beta$ é chamado de logaritmo discreto de β.

Encontrar o logaritmo discreto em $\mathbb{Z}_p$ (onde $\mathbb{Z}_p$ é o conjunto formado pelos inteiros não negativos menores que p, sendo p um número primo) é considerado um problema inacessível quando p possui no mínimo 150 algarismos, assim procederemos o logaritmo discreto limitado a $\mathbb{Z}_p$.

Seja p primo e $a \in \mathbb{Z}$ com a não congruente a zero módulo p. Suponhamos que para cada inteiro b com b não congruente a zero módulo p, exista um inteiro x tal

que

$$a^x \equiv b \bmod p$$

O Problema do Logaritmo Discreto equivale a encontrar o inteiro x para cada b.

Proposição 2.1. *Se existir $x \in \mathbb{Z}$ tal que $a^x \equiv b \bmod p$, então esta congruência possui infinitas soluções em $\mathbb{Z}$.*

Demonstração: Seja x uma solução para a congruência. Pelo Pequeno Teorema de Fermat (P.T.F.), temos que

$$a^{p-1} \equiv 1 \bmod p.$$

Assim, temos que:

$$a^x.a^{p-1} \equiv b.1 \bmod p \Rightarrow a^{x+(p-1)} \equiv b \bmod p,$$

ou seja, $x + (p-1)$ é uma solução da congruência. De modo geral, temos que $x + k(p-1)$ é solução da congruência, $\forall k \in \mathbb{Z}$. De fato:

$$a^{x+k(p-1)} \equiv a^x.a^{k(p-1)} \equiv a^x.(a^{p-1})^k \equiv b.1^k \equiv b \bmod p.$$

Logo, a congruência possui infinitas soluções inteiras.

□

Proposição 2.2. *Dado um inteiro fixo $a \neq 0$, o Problema do Logaritmo Discreto $a^x \equiv b \bmod p$ possui solução em $\mathbb{Z}_p$, com b não congruente a a módulo p, se, e somente se, a é um gerador do grupo multiplicativo $\mathbb{Z}^*{}_p$.* [1]

Demonstração:

[1] Seja p um número primo. Chamamos de grupo multiplicativo $\mathbb{Z}^*{}_p$ ao conjunto $\mathbb{Z}^*{}_p = \{n \in \mathbb{Z}; 0 < n < p$ munido da operação de multiplicação$\}$.

Vamos supor que $a^x \equiv b \bmod p$ possui solução em $\mathbb{Z}_p$ para todo inteiro b. Isto significa que, qualquer que seja b $\in \mathbb{Z}_p$ existe um $x \in \mathbb{Z}_p$ tal que $a^x \equiv b \bmod p$, logo a é um gerador de $\mathbb{Z}^*{}_p$.

Agora vamos supor que a é um gerador de $\mathbb{Z}^*{}_p$. Cada elemento de $\mathbb{Z}_p$ é congruente a alguma potência de a, portanto, $\forall b \in \mathbb{Z}_p$ existe $x \in \mathbb{Z}_p$ tal que $a^x \equiv b \bmod p$, logo, o Problema do Logaritmo Discreto possui solução. □

2.0.1 Protocolo Diffie-Hellman

Podemos perceber que quanto maior for p a resolução do Problema do Logaritmo Discreto torna-se difícil até mesmo para um computador. Foi essa dificuldade que conduziu Diffie e Hellman a criarem um protocolo de encriptação baseado no Problema do Logaritmo Discreto. Em 1946 Diffie e Hellman propõem um modelo que combina criptografia simétrica ao Problema do Logaritmo Discreto para efetuar a troca de chaves. O processo consiste em efetuar a troca de chave para criptografia simétrica por um canal inseguro de tal forma que, mesmo que um terceiro intercepte a chave compartilhada, seja inviável determinar as chaves secretas e, consequentemente, decifrar a mensagem.

Abaixo, estão descritos os passos para a criação e compartilhamento da chave. Para melhor exemplificação denominaremos o emissor de Maria e o receptor de João.

1. Inicialmente, Maria e João escolhem um primo p suficientemente grande e um inteiro g tal que $0 < g < p$ e g seja um gerador de $\mathbb{Z}^*{}_p$. Estes valores p e g são públicos.

2. Maria escolhe um inteiro a, tal que $1 \leq a \leq p-2$, que é secreto.

3. João escolhe um inteiro b, tal que $1 \leq b \leq p-2$, que, também,é secreto.

4. Maria escolhe um inteiro $A \equiv g^a \bmod p$ e o envia para João.

5. João escolhe um inteiro $B \equiv g^b \bmod p$ e o envia para Maria.

6. Maria, então, escolhe uma chave $K_A \equiv B^a \bmod p$.

$$K_A \equiv (g^b)^a \equiv g^{ab} \bmod p.$$

7. João, por sua vez, escolhe uma chave $K_B \equiv A^b \bmod p$.

$$K_B \equiv (g^b)^a \equiv g^{ab} \bmod p.$$

8. A chave secreta compartilhada é um inteiro $K_{AB} \equiv K_A \equiv K_B \bmod p$.

Reparem que Maria e João possuem a mesma chave para codificação e decodificação, mas em nenhum momento esta chave K_{AB} foi transmitida de fato. Após efetuar este procedimento, a comunicação pode ser realizada utilizando um criptossistema (sistema de criptografia, utilizado na encriptação da mensagem, onde o emissor e o receptor já determinam como a mensagem será cifrada e decodificada) de chave secreta qualquer.

Para codificar a mensagem $M \in \mathbf{P}$ deve-se aplicar a função de codificação

$$E_{K_{AB}} : \mathbf{P} \longrightarrow \mathbf{C},$$

$$x \longmapsto K_{AB}.x \bmod p$$

onde:

$\mathbf{P}$ é um conjunto finito de possíveis textos legíveis e;

$\mathbf{C}$ é um conjunto finito de possíveis textos cifrados

à mensagem M, gerando a mensagem cifrada M':

$$M' = E_{K_{AB}}(M) \equiv K_{AB}.M \bmod p.$$

Agora, para decodificar a mensagem $M' \in \mathbf{C}$, aplicamos a função de decodificação a M', ou seja, $D_{K_{AB}}(M')$, que utiliza o inverso de K_{AB} módulo p, ${K_{AB}}^{-1}$.

$$D_{K_{AB}}(M') \equiv K_{AB}^{-1}.M' \bmod p$$

$$D_{K_{AB}}(M') \equiv K_{AB}^{-1}.K_{AB}.M \bmod p$$

$$D_{K_{AB}}(M') \equiv 1.M \bmod p$$

$$D_{K_{AB}}(M') \equiv M \bmod p.$$

Vamos supor que um terceiro consiga interceptar a chave que Maria envia a João, neste caso a única informação sobre a chave de que ele tem conhecimento é

$$A \equiv g^a \bmod p.$$

Assim, ele consegue os inteiros p e g mas não consegue a, e para determinar esse valor, precisa calcular o logaritmo discreto $a = \log_g A \bmod p$ o que é inexecutável.

De modo análogo, se esse terceiro receptasse a transmissão de João a Maria, teria a seguinte informação:

$$B \equiv g^b \bmod p$$

onde ele deve calcular o logaritmo discreto $b = \log_g B \bmod p$,o que também é inexecutável, pois ele não conhece o inteiro b e p é um primo com grande quantidade de algarismos.

2.0.2 Criptossistema de Chave Pública ElGamal

Taher ElGamal em 1985, publicou no artigo *A public key cryptosystem and a signature scheme based on discrete logarithms,* um criptossistema de chave pública baseado no Problema do Logaritmo Discreto, onde ElGamal utiliza chaves assimétricas.

Definição 2.3. *Seja p um primo, $g \in \mathbb{Z}_p$ um gerador de $\mathbb{Z}^*{}_p$ e $a \in \mathbb{Z}_p$. Seja $\boldsymbol{P} = \mathbb{Z}_p$ e $\boldsymbol{C} = \mathbb{Z}_p \times \mathbb{Z}_p$ e*

$$K = (p, g, a, A) : A \equiv g^a \ mod\ p$$

(K é um conjunto finito com todas as possíveis chaves de codificação)

Para cada $K = (p, g, a, A)$ *e para cada número aleatório* k*, com* $0 < k < p - 1$*, defina, para cada* $x \in \boldsymbol{P}$

$$E_K(x) = (y_1, y_2),$$

com

$$y_1 \equiv g^k \ mod\ p$$

$$y_2 \equiv xA^k \ mod\ p$$

e para $y_1, y_2 \in \mathbb{Z}_p$*:*

$$D_K(y_1, y_2) = y_2(y_1^a)^{-1} \ mod\ p.$$

Chamamos Criptossistema de Chave Pública ElGamal em $\mathbb{Z}_p$ *à quíntupla*

$$(\boldsymbol{P}, \boldsymbol{C}, K, E_K(x), D_K(y_1, y_2)).$$

Abaixo, está exemplificado o envio da mensagem M de João para Maria. Para isto, Maria e João estabelecem um primo p convenientemente longo e um inteiro g, gerador de $\mathbb{Z}^*{}_p$, sendo que estes valores são públicos. Assim, a comunicação decorre da seguinte forma:

1. Maria escolhe uma chave secreta a, com $1 \leq a \leq p - 2$ e escolhe um inteiro A tal que

$$A \equiv g^a \bmod p.$$

2. Maria envia A para João, que escolhe um inteiro aleatório k e escolhe dois inteiros y_1 e y_2 tais que

$$y_1 \equiv g^k \bmod p \text{ e } y_2 \equiv M.A^k \bmod p.$$

3. João envia o par (y_1, y_2), esta é a mensagem cifrada.

Observe que no passo 1, o valor a escolhido por Maria precisa ser diferente de $p-1$ pois, $g^{\phi(p)} \equiv 1 \bmod p$ e como $\phi(p) = p-1$, teríamos $A \equiv g^{p-1} \equiv 1 \bmod p$, logo, y_2 seria a própria mensagem M e não faria sentido cifrar esta mensagem. Pelo mesmo motivo, deve-se ter $k < p-1$.

Caso um terceiro consiga o valor de A, considerando que p e g são conhecidos, precisa solucionar $\log_g A \bmod p$ para obter a chave secreta a o que é inviável. Além disso se ele interceptar a mensagem (y_1, y_2), deverá determinar $k = \log_g y_1 \bmod p$, o que também é inviável.

Para decodificar a mensagem (y_1, y_2) recebida, Maria deve realizar os seguintes passos:

1. Determinar $x \equiv y_1^a \bmod p$ e seu inverso $x^{-1} \bmod p$.

2. Calcular $y_2.x^{-1}$ para encontrar a mensagem original:

$$\begin{aligned} y_2x^{-1} &\equiv (M.A^k)x^{-1} \equiv M(g^a)^k x^{-1} \equiv M(g^k)^a x^{-1} \\ &\equiv M(y_1)^a x^{-1} \equiv M.x.x^{-1} \equiv M \bmod p. \end{aligned}$$

Assim, depois de realizar estas operações Maria consegue ler a mensagem original.

Para a codificação de um texto, normalmente utiliza-se a Tabela ASCII (Disponível em: <https://www.oficinadanet.com.br> acessado: 21/04/2019.) para modificar a mensagem em um valor numérico, para efetuar as operações necessárias para codificação e decodificação, veja figura 2.1.

Tabela ASCII (códigos de caracteres 0 - 127)

000	016 ▶	032	048 0	064 @	080 P	096 `	112 p
001 ☺	017 ◀	033 !	049 1	065 A	081 Q	097 a	113 q
002 ☻	018 ↕	034 "	050 2	066 B	082 R	098 b	114 r
003 ♥	019 ‼	035 #	051 3	067 C	083 S	099 c	115 s
004 ♦	020 ¶	036 $	052 4	068 D	084 T	100 d	116 t
005 ♣	021 §	037 %	053 5	069 E	085 U	101 e	117 u
006 ♠	022 ▬	038 &	054 6	070 F	086 V	102 f	118 v
007	023 ↨	039 '	055 7	071 G	087 W	103 g	119 w
008	024 ↑	040 (	056 8	072 H	088 X	104 h	120 x
009	025 ↓	041)	057 9	073 I	089 Y	105 i	121 y
010	026 →	042 *	058 :	074 J	090 Z	106 j	122 z
011 ♂	027 ←	043 +	059 ;	075 K	091 [	107 k	123 {
012 ♀	028 ∟	044 ,	060 <	076 L	092 \	108 l	124 |
013	029 ↔	045 -	061 =	077 M	093]	109 m	125 }
014 ♫	030 ▲	046 .	062 >	078 N	094 ^	110 n	126 ~
015 ☼	031 ▼	047 /	063 ?	079 O	095 _	111 o	127 ⌂

Figura 2.1: Tabela ASCII

CAPÍTULO 3

CRIPTOGRAFIA

A criptografia é um método matemático que tem como objetivo codificar uma mensagem de modo que somente o destinatário legítimo consiga decifrá-la. Como foi dito na introdução deste trabalho, a palavra criptografia procede do grego cryptos que significa "secreto , oculto" e é utilizada em várias situações do nosso dia-a-dia.

Os indícios são de que a criptografia começou a ser usada desde a antiguidade. César foi o primeiro a utilizar a criptografia como meio de esconder informações secretas com uma técnica simples, porém eficiente para época, que consiste em substituir uma letra pela outra transladando o alfabeto um número fixo de vezes. Essa técnica passou a ser chamada de Cifra de César, em homenagem ao criador.

Exemplo 3.1. *Transladando o alfabeto duas posições temos que a palavra CESAR ficaria: EGUCT.*

É claro que esse código de Cesar é muito fácil de se decifrar, assim como qualquer outro código que envolve substituição de letras, pois a frequência média em que cada letra é utilizada em sua língua é constante.

No decorrer dos anos a criptografia foi se adaptando de modo a se tornar mais difícil de decifrar. Porém juntamente com os anos, a humanidade foi se aperfeiço-

ando em tecnologias tendo um grande aliado para decifrar os códigos secretos: o computador. Contudo, tornou-se essencial criar novos códigos, que fossem difíceis de decifrar mesmo com a ajuda de um computador.

Neste capítulo estudaremos o RSA que é o método de criptografia de chave pública mais conhecido universalmente. Pautamos este capítulo nos trabalhos [1],[2] e [3]

3.1 Criptografia RSA

O mais conhecido dos métodos de criptografia de chave pública é o RSA, que foi inventado por dois cientistas da computação que trabalhavam no MIT(Instituto de Tecnologia de Massachusetts) Ronald Rivest e Adi Shamir, que estavam empenhados em criar um método de criptografia de chave assimétrica eficiente. Foi ajudado pelo matemático Leonard Adleman. O método foi patenteado em 1978 pelos três, onde o nome RSA procede das iniciais dos três inventores.

Todo processo deste método é composto em duas etapas básicas: a codificação de mensagem e a decodificação da mensagem codificada. Decodificar é o processo que um destinatário legítimo do código faz para ler a mensagem. Já decifrar significa ler uma mensagem codificada podendo ser um terceiro destinatário (não ser um destinatário legítimo). A execução desse método de criptografia depende de dois primos distintos grandes que chamaremos de p e q. Para codificar uma mensagem usando o método RSA devemos conhecer a chave de decodificação (que é pública) que é o produto $n = pq$. O processo de decodificação só é possível quando conhecemos os números p e q.

Neste capítulo estudaremos o método RSA e citaremos alguns exemplos de como criptografar usando o método, para isso não iremos utilizar números grandes e sim números que são possíveis de manusear com calculadora científica.

3.1.1 Exposição do método RSA

Antes de entrarmos na fase da codificação devemos realizar a pré-codificação, que consiste em transformar a mensagem em uma sequência de números. Para tal, cada letra do alfabeto será representada por um número de dois algarismos para evitar dubiedades. Por exemplo, se fizéssemos A equivaler ao número 1, B ao número 2, e assim sucessivamente, não teríamos como saber se 12 representa AB ou L (que é a décima segunda letra do alfabeto). Para realizar a pré-codificação, transforma-se letras em números usando a seguinte tabela:

Tabela 3.1: Tabela de conversão RSA

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: A autora.

Exemplo 3.2. *A palavra:*

Matemática

convertida em números ficaria 22102914221029181210.

Em caso de frases, o espaçamento entre palavras será substituído pelo número 99.

Exemplo 3.3. *A frase:*

Amo Matemática

convertida em números ficaria 10222499221029142210291812 10.

Após a conversão da mensagem em números, deve-se "quebrar"esse número em blocos menores que o número $n = pq$. Para isso devemos escolher dois números primos distintos p e q.

Exemplo 3.4. *Se escolhermos* $p = 11$ *e* $q = 13$*, então* $n = 143$*. Logo, cada bloco da mensagem deve ser menor que 143. Quebrando em blocos a mensagem MATEMÁTICA temos:*

$$22 - 10 - 29 - 14 - 22 - 10 - 29 - 18 - 12 - 10$$

Não há regras para escolhermos os blocos em que vamos dividir a mensagem, porem devemos tomar alguns cuidados. Como mencionado anteriormente, nenhum bloco deve ser maior que o número n. Assim a mensagem MATEMÁTICA também pode ser quebrada da seguinte forma:

$$22 - 102 - 91 - 4 - 22 - 10 - 29 - 18 - 12 - 10$$

Também não podemos começar o bloco com o número zero porque isto traria problemas na hora de decodificar. É por isso que não escolhemos os blocos:

$$221 - 02 - 91 - 42 - 21 - 029 - 18 - 12 - 10$$

Aqui, encerramos a etapa da pré-codificação.

Codificação

Para esta etapa, precisamos de n, que é o produto dos primos p e q e de um número inteiro positivo e que seja inversível módulo $\phi(n)$, ou seja, $mdc(e, \phi(n)) = 1$. Como p e q são primos, sabemos que:

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

Assim, o par (n, e) é a chave de codificação do sistema RSA. Na etapa da pré-codificação a mensagem numérica foi separada em vários blocos, codificaremos cada bloco isoladamente, e a mensagem codificada será a sequência dos blocos codificados.

Aqui, os blocos codificados não poderão ser agrupados de modo a formar longos números. Chamaremos de $C(b)$, o bloco codificado. Para calcular $C(b)$ devemos obter o resto da divisão de b^e por n, em outras palavras:

$$b^e \equiv C(b) \text{ mod n.}$$

Decodificação

Para decodificar um bloco precisamos de dois números: n e o inverso de e em $\phi(n)$, que chamaremos de d. Assim, o par (n, d) será a chave de decodificação. Seja $D(C(b))$ o processo de decodificação. Para obter $D(C(b))$ devemos calcular o resto da divisão de $(C(b))^d$ por n, em outras palavras, devemos obter:

$$D(C(b)) \equiv b \text{ mod n.}$$

Para tanto, recordemos alguns resultados já estudados. Sendo b um inteiro, relativamente primo com n, o Teorema de Euler nos diz que:

$$b^{\phi(n)} \equiv 1 \text{ mod n.}$$

Como p e q são primos, pelas propriedades da função Totiente de Euler, temos que

$$\phi(p) = p - 1 \text{ e } \phi(q) = q - 1,$$

então

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

Para decifrar a mensagem é fundamental encontrar um inteiro d tal que $ed \equiv 1 \text{ mod}(\phi(n))$ o que implica em $ed \equiv 1 \text{ mod}((p-1)(q-1))$ e isto, pelo Teorema de

Euler, implica em:

$$d \equiv e^{\phi((p-1)(q-1))-1} \text{ mod((p-1)(q-1))}.$$

Portanto de $ed \equiv 1 \text{ mod}(\phi(n))$ concluímos que existe um inteiro k tal que $ed \equiv k\phi(n) + 1$ de onde segue que:

$$b \equiv b.1 \equiv b(1)^k \equiv b(b^{\phi(n)})^k \equiv b^{k\phi(n)+1} \text{ mod } n$$

e

$$b^{k\phi(n)+1} \equiv b^{ed} \equiv (b^e)^d \equiv (\text{C(b)})^d \text{ mod } n.$$

Por tanto

$$D(C(b)) \equiv (C(b))^d \text{ mod } n.$$

Observe que $D(C(b))$ é a relação inversa de $C(b)$.

3.2 Exemplo de uma mensagem criptografada usando o RSA

Vamos codificar e decodificar a mensagem AMO MATEMÁTICA de acordo com o sistema RSA. Usaremos para a chave pública o par $(n, e) = (143, 7)$.

3.2.1 Pré - Codificação

Vamos transformar cada letra da mensagem AMO MATEMÁTICA em números de dois algarismo, de acordo com a tabela de conversão RSA (desconsiderando o acento agudo). Logo a frase codificada ficaria:

10222499221029142210291812 10.

Agora quebramos o bloco inteiro em blocos menores. Para isso devemos tomar

alguns cuidados. Como já foi dito não podemos escolher blocos maiores que o número n, e não devemos iniciar o bloco com o número zero. A mensagem atual pode ser quebrada assim:

$$102 - 22 - 49 - 92 - 2 - 10 - 29 - 14 - 22 - 102 - 91 - 81 - 2 - 10.$$

Encerrada a etapa da pré-codificação passaremos a etapa da codificação.

3.2.2 Codificação

Como $e = 7$ e chamando cada bloco codificado de $C(b)$, a regra para a codificação é a seguinte:

$$C(b) = \text{resto da divisão de } b^7 \text{ por } 143$$

ou seja,

$$b^7 \equiv C(b) \bmod 143.$$

Realizando as contas temos:

- $102^7 \equiv (102^3)^2.102 \equiv (5)^2.102 \equiv 25.102 \equiv 2550 \equiv 119 \bmod 143$;
- $22^7 \equiv (22^2)^3.22 \equiv (55)^3.22 \equiv (55)^2.55.22 \equiv 22.55.22 \equiv (22)^2.55 \equiv (55)^2 \equiv 22 \bmod 143$;
- $49^7 \equiv (49^3)^2.49 \equiv (103)^2.49 \equiv 27.49 \equiv 1323 \equiv 36 \bmod 143$;
- $92^7 \equiv (92^2)^3.92 \equiv (27)^3.92 \equiv 92.92 \equiv (92)^2 \equiv 27 \bmod 143$;
- $2^7 \equiv 128 \bmod 143$;
- $10^7 \equiv (10^2)^3.10 \equiv (-43)^3.10 \equiv (-43)^2.(-43).10 \equiv 133.(-430) \equiv (-10).(-430) \equiv (10).(430) \equiv 10.1 \equiv 10 \bmod 143$;
- $29^7 \equiv (29^3)^2.29 \equiv (79)^2.29 \equiv 6241.29 \equiv 92.29 \equiv 2668 \equiv 94 \bmod 143$;
- $14^7 \equiv (14^3)^2.14 \equiv (27)^2.14 \equiv 729.14 \equiv (14)^2 \equiv 53 \bmod 143$;

- $22^7 \equiv (22^2)^3.22 \equiv (55)^3.22 \equiv (55)^2.55.22 \equiv 22.55.22 \equiv (22)^2.55 \equiv (55)^2 \equiv 22 \bmod 143$;
- $102^7 \equiv (102^3)^2.102 \equiv (5)^2.102 \equiv 25.102 \equiv 2550 \equiv 119 \bmod 143$;
- $91^7 \equiv (91^3)^2.91 \equiv (104)^2.91 \equiv 91.91 \equiv (91)^2 \equiv 130 \bmod 143$;
- $81^7 \equiv (81^3)^2.81 \equiv (53)^2.81 \equiv 92.81 \equiv 7452 \equiv 16 \bmod 143$;
- $2^7 \equiv 128 \bmod 143$;
- $10^7 \equiv (10^2)^3.10 \equiv (-43)^3.10 \equiv (-43)^2.(-43).10 \equiv 133.(-430) \equiv (-10).(-430) \equiv (10).(430) \equiv 10.1 \equiv 10 \bmod 143$.

Reunindo os blocos temos a seguinte mensagem codificada:

$$119 - 22 - 36 - 27 - 128 - 10 - 94 - 53 - 22 - 119 - 130 - 16 - 128 - 10.$$

Lembrando que após a codificação dos blocos não podemos agrupar novamente os números formados em um só bloco, pois a decodificação da mensagem está relacionado a cada resto. Por exemplo, três blocos que originalmente seriam $11 - 21 - 33$, agrupados, formariam o número 221533 que poderia ser interpretado pelos blocos $112 - 133$ que também são restos possíveis para $p = 143$. Encerrada a etapa da codificação passaremos a decodificação.

3.2.3 Decodificação

Para decodificar uma mensagem codificada precisamos de dois números: n e o inverso de d maior que zero de 7 módulo $(p-1)(q-1)$, onde p e q sã os únicos fatores primos de n. Como $p = 11$ e $q = 13$ (pois $143 = 11.13$), para calcular d devemos calcular:

$$7.d \equiv 1 \bmod ((p-1)(q-1))$$

$$7.d \equiv 1 \text{ mod } ((11-1)(13-1))$$

$$7.d \equiv 1 \text{ mod } 120.$$

Aplicando o resultado

$$d \equiv e^{\phi((p-1)(q-1))-1} \text{ mod } ((p-1)(q-1)),$$

temos

$$q \equiv 3^{\phi(120)-1} \text{ mod } 120.$$

Como $\phi(120) = \phi(8).\phi(3).\phi(5) = 4.2.4 = 32$, segue que:

$$d \equiv 7^{32-1} \equiv 7^{31} \equiv 103 \text{ mod } 120.$$

Temos, então, que $d = 103$ é o menor inteiro positivo que é solução da congruência dada. Assim, o par $(n, d) = (143, 103)$ é a chave de decodificação, tal chave só pode ser obtida por quem tem a função de receber a mensagem. Agora que conhecemos o par $(nd,)$, a regra para a decodificação será:

$$D(a) = \text{ resto da divisão de } a^d \text{ por n}$$

Em outras palavras:

$$a^d \equiv D(a) \text{ mod } n$$

Lembrando que a é o bloco codificado e $D(a)$ será o resultado do processo de decodificação. Realizando as contas temos:

- $119^{103} \equiv (119^2)^{51}.(119) \equiv (4)^{51}.(119) \equiv (4^{10})^5.(4).(119) \equiv (100)^5.(476) \equiv (100^2)^2.(100).(47) \equiv (133)^2.(4700) \equiv (100).(124) \equiv 12400 \equiv 102 \text{ mod } 143$;
- $22^{103} \equiv (22^2)^{51}.(22) \equiv (55)^{51}.(22) \equiv (55^2)^{25}.(55).(22) \equiv (22)^{25}.(1210) \equiv (22^2)^{12}.(22).(66) \equiv (55)^{12}.(1452) \equiv (55^2)^6.(22) \equiv 22^6(22) \equiv (22^2)^3.(22) \equiv (55)^2.(55).(22) \equiv (22).(22).(55) \equiv 22^2.(55) \equiv 55^2 \equiv 22 \text{ mod } 143$;

- $36^{103} \equiv (36^2)^{51}.(36) \equiv (9^3)^{17}.(36) \equiv 729^{17}.(36) \equiv (14)^{17}.(36) \equiv (14^2)^8.(14).(36) \equiv (53)^8.(504) \equiv (53^2)^4.(75) \equiv 92^4.(75) \equiv (92^2)^2.(75) \equiv (27)^2.(75) \equiv (14).(75) \equiv 1050 \equiv 49 \bmod 143$;

- $27^{103} \equiv (27^2)^{51}.(27) \equiv (14)^{51}.(27) \equiv (14^2)^{25}.(14).(27) \equiv (53)^{25}.(378) \equiv (53^2)^{12}.(53).(92) \equiv (92)^{12}.(4876) \equiv (92^2)^6.(14) \equiv 27^6.(14) \equiv (27^2)^3.(14) \equiv (14)^3.(14) \equiv (14^2).(14^2) \equiv (53).(53) \equiv 53^2 \equiv 92 \bmod 143$;

- $128^{103} \equiv (128^2)^{51}.(128) \equiv (82)^{51}.(128) \equiv (82^2)^{25}.(82).(128) \equiv (3)^{25}.(10496) \equiv (3^5)^5.(57) \equiv (243)^5.(57) \equiv (100^2)^2.(100).(57) \equiv 133^2.(5700) \equiv (100).(123) \equiv 12300 \equiv 2 \bmod 143$;

- $10^{103} \equiv (10^3)^{34}.(10) \equiv (142)^{34}.(10) \equiv (142^2)^{17}.(10) \equiv (1)^{17}.10 \equiv 10 \bmod 143$;

- $94^{103} \equiv (94^2)^{51}.(94) \equiv (113)^{51}.(94) \equiv (113^2)^{25}.(113).(94) \equiv (42)^{25}.(10622) \equiv (42^2)^{12}.(42).(40) \equiv (48)^{12}.(1680) \equiv (48^2)^6.(107) \equiv 16^6.(107) \equiv (16^2)^3.(107) \equiv (113)^2.(113).(107) \equiv (42).(12091) \equiv (42).(79) \equiv 3318 \equiv 29 \bmod 143$;

- $53^{103} \equiv (53^2)^{51}.(53) \equiv (92)^{51}.(53) \equiv (92^2)^{25}.(92).(53) \equiv (27)^{25}.(4876) \equiv (27^2)^{12}.(27).(14) \equiv (14)^{12}.(378) \equiv (14^2)^6.(92) \equiv 53^6.(92) \equiv (53^2)^3.(92) \equiv (92)^3.(92) \equiv (92^2).(92^2) \equiv (27).(27) \equiv 27^2 \equiv 14 \bmod 143$;

- $119^{103} \equiv (119^2)^{51}.(119) \equiv (4)^{51}.(119) \equiv (4^{10})^5.(4).(119) \equiv (100)^5.(476) \equiv (100^2)^2.(100).(47) \equiv (133)^2.(4700) \equiv (100).(124) \equiv 12400 \equiv 102 \bmod 143$;

- $130^{103} \equiv (130^2)^{51}.(130) \equiv (26)^{51}.(130) \equiv (26^2)^{25}.(26).(130) \equiv (104)^{25}.(3380) \equiv (104^2)^{12}.(104).(91) \equiv (91)^{12}.(9464) \equiv (91^2)^6.(26) \equiv 130^6(26) \equiv (130^2)^3.(26) \equiv (26)^3.(26) \equiv 26^2.26^2 \equiv (104).(104) \equiv 10816 \equiv 91 \bmod 143$;

- $16^{103} \equiv (16^2)^{51}.(16) \equiv (113)^{51}.(16) \equiv (113^2)^{25}.(113).(16) \equiv (42)^{25}.(1808) \equiv (42^2)^{12}.(42).(92) \equiv (48)^{12}.(3864) \equiv (48^2)^6.(3) \equiv 16^6(3) \equiv (16^2)^3.(3) \equiv (113)^2.(113).(3) \equiv (42).(339) \equiv (42).(53) \equiv 2226 \equiv 81 \bmod 143$.

Agrupando os blocos decodificados, formamos novamente o número 1022249922102914221029181, que, de acordo com a convenção da Tabela de conversão RSA, significa AMO MATEMÁTICA.

Decodificar um bloco da mensagem codificada é encontrar o bloco correspondente da mensagem original, ou seja, $D(C(b)) = b$, sem isto não teríamos código algum.

Outra maneira de decodificar o bloco codificado é realizar os cálculos com a ajuda dos Teoremas de Fermat e da resolução de sistemas de congruências. Sabemos que devemos calcular o resto da divisão de 119^{103} por $n = 143$. Calculamos 119^{103} modulo 11 e 119^{103} modulo 13 que são primos em que n se fatora. Inicialmente, temos :

$$119 \equiv 9 \bmod 11 \tag{3.2.1}$$

e

$$119 \equiv 2 \bmod 13. \tag{3.2.2}$$

Assim, de (3.2.1) temos:

$$119^{103} \equiv 9^{103} \bmod 11.$$

Pelo Teorema de Fermat sabemos que :

$$9^{10} \equiv 1 \bmod 11.$$

Como

$$103 = 10.10 + 3,$$

segue que

$$119^{103} \equiv 9^{10.10+3} \equiv (9^{10})^{10}.9^3 \equiv 1^{10}.9^3 \equiv 9^3 \equiv 3 \bmod 11$$

. Da equação (3.2.2), temos que :

$$119^{103} \equiv 2^{103} \bmod 13.$$

Pelo Teorema de Fermat temos:

$$2^{12} \equiv 1 \bmod 13.$$

Como

$$103 = 12.8 + 7,$$

segue que

$$119^{103} \equiv 2^{12.8+7} \equiv (2^{12})^8.2^7 \equiv 1^8.2^7 \equiv 2^7 \equiv 11 \bmod 13.$$

Assim chamando 119^{103} de X, temos que

$$X \equiv 3 \bmod 11$$

$$X \equiv 11 \bmod 13.$$

Resolvemos este sistema de equações utilizando o Algarismo Chinês dos Restos, da primeira equação temos que, existe $Y \in \mathbb{Z}$, tal que:

$$X \equiv 11Y + 3.$$

Substituindo X na segunda equação, temos:

$$11y + 3 \equiv 11 \bmod 13 \text{ que resulta em } Y = 9 \bmod 13.$$

Logo, existe $K \in \mathbb{Z}$, tal que:

$$Y = 13K + 9$$

Voltando, a equação $X \equiv 11Y + 3$ e substituindo o valor de Y temos:

$$X = 11(13K + 9) + 3 \Rightarrow X \equiv 143K + 102.$$

Onde 102 é a menor solução positiva para o sistema e também o bloco inicial procurado. Procedendo da mesma maneira com os blocos restantes, podemos obter a

mensagem inicial.

Afirmamos anteriormente, antes de codificarmos a mensagem, que não poderíamos "quebrar"o número por blocos que começam com o número zero, vamos verificar o porquê.

Vamos codificar e decodificar a palavra ALUNO. Aqui utilizaremos a chave pública $(n, e) = (253, 3)$. Realizando a pré-codificação temos:

$$1021302324.$$

Vamos quebrar o bloco inteiro em blocos menores, colocando o número zero no início de um bloco para analisá-lo. Podemos quebrá-lo da seguinte forma:

$$1 - 021 - 30 - 232 - 4$$

Como $e = 3$, e cada bloco codificado é representado por $C(b)$, a regra para a codificação é a seguinte:

$$C(b) = \text{ resto da divisão de } b^3 \text{ por } 253,$$

ou seja,

$$b^3 \equiv C(b) \bmod 253.$$

Realizando as contas temos:

- $1^3 \equiv 1 \bmod 253$;
- $21^3 \equiv (21^2).21 \equiv 188.91 \equiv 3948 \equiv 153 \bmod 253$;
- $30^3 \equiv (30^2).30 \equiv 141.30 \equiv 4230 \equiv 182 \bmod 253$;
- $232^3 \equiv (232^2).232 \equiv 188.232 \equiv 43616 \equiv 100 \bmod 253$;
- $4^3 \equiv 64 \bmod 253$.

Reunindo os blocos temos a seguinte mensagem codificada:

$$1 - 153 - 182 - 100 - 64.$$

Agora para decodificar a mensagem obtida, primeiro devemos calcular o inverso de d maior que zero de 3 módulo $(p-1)(q-1)$. Como $p = 11$ e $q = 23$ pois $(11.23 = 253)$, para calcular d temos:

$$d \equiv 3^{\phi(220)-1} \bmod 220.$$

Como $\phi(220) = \phi(10).\phi(23) = 4.10 = 40$, segue que

$$d \equiv 3^{40-1} \equiv 3^{39} \equiv 147 \bmod 220$$

Logo, devemos calcular o resto da divisão de a^{147} por 253, realizando as contas temos:

- $1^{147} \equiv 1 \bmod 253$;
- $153^{147} \equiv (153^2)^{73}.(153) \equiv (133^2)^{36}.(133).(153) \equiv (232^2)^{18}.(20349) \equiv (188^2)^9.(109) \equiv (177^2)^4.(177).(109) \equiv (210)^4.(19293) \equiv (78).(78).(65) \equiv (78^2).65 \equiv 12.65 \equiv 780 \equiv 21 \bmod 253$;
- $182^{147} \equiv (182^2)^{73}.(182) \equiv (234^2)^{36}.(234).(182) \equiv (108^2)^{18}.(42588) \equiv (108^2)^{18}.(84) \equiv (26^2)^9.(84) \equiv (170^2)^4.(170).(84) \equiv (58^2).(58^2).14280 \equiv 75.75.112 \equiv 59.112 \equiv 6608 \equiv \bmod 253$;
- $100^{147} \equiv (100^2)^{73}.(100) \equiv (133^2)^{36}.(133).(100) \equiv (232^{36}).(13300) \equiv (232^2)^{18}.(144) \equiv (188^2)^9.(144) \equiv (177^2)^4.(177).(144) \equiv (210^4).25488 \equiv (210^2).(210^2).188 \equiv (78).(78).(188) \equiv (6084).(188) \equiv (12).(188) \equiv 2256 \equiv 232 \bmod 253$;
- $64^{147} \equiv (64^2)^{73}.(64) \equiv (48^2)^{36}.(48).(64) \equiv (27^2)^{18}.(3072) \equiv (223^{18}).(36) \equiv (223^2)^9.(36) \equiv (141^2)^4.(141).(36) \equiv (147^4).5076 \equiv (147^2).(147^2).16 \equiv (104).(104).(16) \equiv$

$$173056 \equiv 4 \bmod 253.$$

Agrupando os blocos temos:

$$121302324,$$

que convertida em texto, se torna

$$CD?NO$$

Que não corresponde à mensagem original.

Assim encerramos nossa seção de exemplificação do método RSA.

3.2.4 Segurança

Sabemos que o RSA é um método de chave pública. Dados dois números inteiros primos, os parâmetros do sistema que estamos utilizando e $n = p.q$. A chave de codificação coincide com a chave pública do sistema. Assim, o par (n, e) é disponível a qualquer usuário. O que torna o RSA seguro está na complexidade de calcular d quando apenas n e e são conhecidos, pois muitas operações são envolvidas no processo.

Pelos estudos, só sabemos encontrar d utilizando o algoritmo euclidiano estendido a $\phi(n)$ e e. Por outro lado, só sabemos encontrar $\phi(n)$ se soubermos fatorar n para obter p e q. Assim, só conseguimos desvendar o código se fatorarmos n, o que é um problema muito difícil se n for grande, pois não conhecemos algoritmos rápidos de fatoração. Chamaremos a tentativa de desvendar uma chave privada de "ataque", os ataques comuns ao RSA são os Ataques Matemáticos e a Força Bruta.

O ataque de Força Bruta equivale em tentar todas as combinações de chaves possíveis até conseguir decifrar a mensagem, tornando-a inviável pois a chave é muito grande e exige um nível de processamento altíssimo para utilizar todas as combinações em um tempo mais curto. Assim, o ataque a Força Bruta não é algo para se

preocupar. Quanto ao Ataque Matemático, vamos supor que, alguém inventou uma maneira de encontrar d sem ter que fatorar n. Por exemplo, o que aconteceria se criasse um algoritmo rápido para calcular $\phi(n)$ a partir de n e e? Assim, teríamos conquistado um algoritmo rápido de fatoração. O que estamos considerando é que $n = pq$ e $\phi(n) = (p-1)(q-1)$ são ambos conhecidos. Queremos obter p e q a partir disso. Contudo,

$$\phi(n) \equiv (p-1)(q-1) = p.q - (p+q) + 1 = n - (p+q) + 1,$$

de forma que $p + q = n - \phi(n) + 1$ é conhecido. Entretanto

$$(p+q)^2 - 4n = (p^2 + q^2 + 2pq) - 4pq = (p-q)^2$$

Logo,

$$p - q = \sqrt{(p+q)^2 - 4n}$$

também é conhecido. Mas conhecendo $p+q$ e $p-q$ calculamos facilmente p e q, ou seja, fatoramos n.

Acabamos de ver que não adianta alguém inventar uma máquina de encontrar $\phi(n)$ sem fatorar n, pois conhecendo os dois chegamos aos fatores de n. E caso alguém invente um algoritmo que ache d a partir de n e e, como $e.d \equiv 1 \bmod \phi(n)$, isto implica que conhecemos um múltiplo de $\phi(n)$, o que é suficiente para fatorar n, mas a demonstração está fora de cogitação.

Resta idealizar que é possível encontrar b a partir da forma reduzida de b^e módulo n sem tentar encontrar d. Além de uma técnica de acessível tentativa-impraticável quando n é grande, ninguém até agora conseguiu tal método. Diante do pressuposto, quebrar o RSA e fatorar n são problemas similares, ainda que isto não tenha sido demonstrado.

CAPÍTULO 4

CRIPTOGRAFIA COM O USO DE CURVAS ELÍPTICAS

Neste capítulo falaremos sobre a criptografia com uso de curvas elípticas. Essa técnica foi, inicialmente, introduzida em 1985 por Victor Miller e Neal Koblitz e foi abordada no uso de curvas elípticas como uma nova forma de implementação a um sistema de chave pública em algumas das aplicações já existentes.

Esse método criptográfico tem tido uma relevância nas últimas décadas pois está associado a crescente necessidade de segurança nos modernos meios de comunicação, fundamentado em computadores onde a eficiência de processamento tem evoluído a cada instante.

Neste capítulo serão apresentados os conceitos matemáticos usados no sistema de criptografia desenvolvido a partir das curvas elípticas definidas sobre corpos finitos. Para tal assumiremos que o leitor tenha conhecimento de alguns conceitos apresentados em disciplinas do curso de graduação em matemática tais como grupos, anéis, corpos, etc. O referencial teórico empregado neste capítulo pode ser averiguado nas obras de [6], [5], [7] e [8].

4.1 Definição de uma Curva Elíptica

Curvas elípticas são definidas a partir da Equação de Weierstrass sobre um corpo $\mathbb{K}$:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

com $a, b, c, d, e \in \mathbb{K}$ mais, um ponto chamado de ponto no infinito (representaremos esse ponto por ∞). Neste trabalho, trabalharemos com curvas elípticas simétricas em relação ao eixo das abcissas e sem singularidades. Assim, trabalharemos com uma versão simplificada da Equação de Weierstrass.

Definição 4.1. *Seja $\mathbb{K}$ um corpo. Uma curva elíptica E sobre $\mathbb{K}$, denotada por $E(\mathbb{K})$, é o lugar geométrico dos pontos $(x, y) \in \mathbb{K} \times \mathbb{K}$ tais que x e y são soluções da equação*

$$y^2 = x^3 + ax + b$$

com $a, b \in \mathbb{K}$ e $4a^3 + 27b^2 \neq 0$.

Esta curva não possui raízes múltiplas, ou seja, deve ser uma curva não-singular, por isso devemos ter $\triangle = 4a^3 + 27b^2 \neq 0$.

Alguns gráficos de curvas elípticas são ilustrados nas Figuras 4.1 e 4.2.

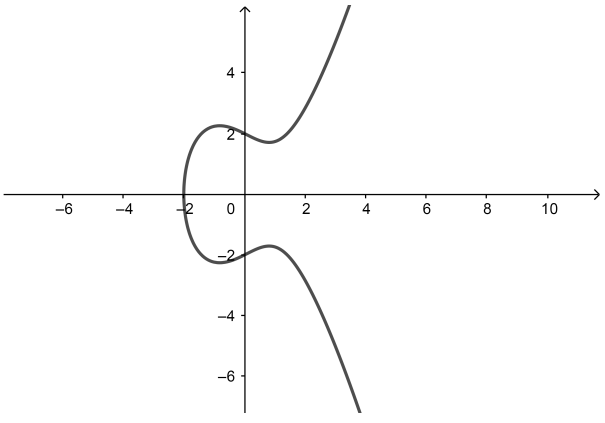

Figura 4.1: Gráfico da curva $y^2 = x^3 - 2x + 4$

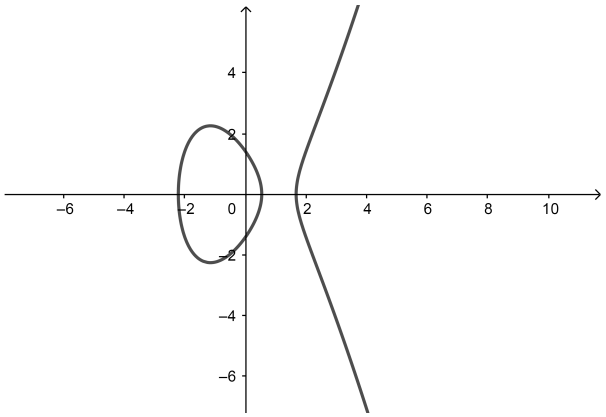

Figura 4.2: Gráfico da curva $y^2 = x^3 - 4x + 2$

Esses gráficos são de curvas definidas para os reais, ou seja, os valores das variáveis x e y na equação são reais e os valores dos parâmetros a e b são números reais. Porém uma curva elíptica pode ser definida em qualquer corpo. Neste capítulo, estamos interessados no caso onde estão definidas sobre corpos finitos.

Queremos definir uma estrutura de grupo no conjunto das curvas elípticas, para isso vamos definir a "soma"entre dois pontos. Essa soma pode ser tratada tanto de forma geométrica ou algébrica, iremos, inicialmente, analisar a forma geométrica. O ponto infinito, ∞, que mencionamos anteriormente será o nosso elemento neutro da operação. Assim, se Ω é uma curva elíptica sobre um corpo K, e temos $P \in \Omega$, então:

$$P + \infty = P = \infty + P.$$

Consideremos o simétrico de um ponto $P = (x, y)$ sendo o ponto $-P = (x, -y)$, se somarmos um ponto $P \in \Omega$ com o ponto simétrico $-P$, obtemos o ponto infinito, logo:

$$P + (-P) = \infty = (-P) + P.$$

Tome dois pontos P e Q distintos de uma curva elíptica sobre o corpo $\mathbb{R}$ dos números reais, seja PQ o segmento de reta que interceptará a curva em um terceiro

ponto que chamaremos de R' (estamos considerando o caso em que a reta não seja vertical). Assim, o reflexo do ponto R' em relação ao eixo horizontal, que é dado por R, será a soma de P e Q. Logo:

$$R = P + Q.$$

A figura 4.3, representa graficamente a soma entre dois pontos distintos $P, Q \in \Omega$ em uma curva elíptica sobre o corpo $\mathbb{R}$.

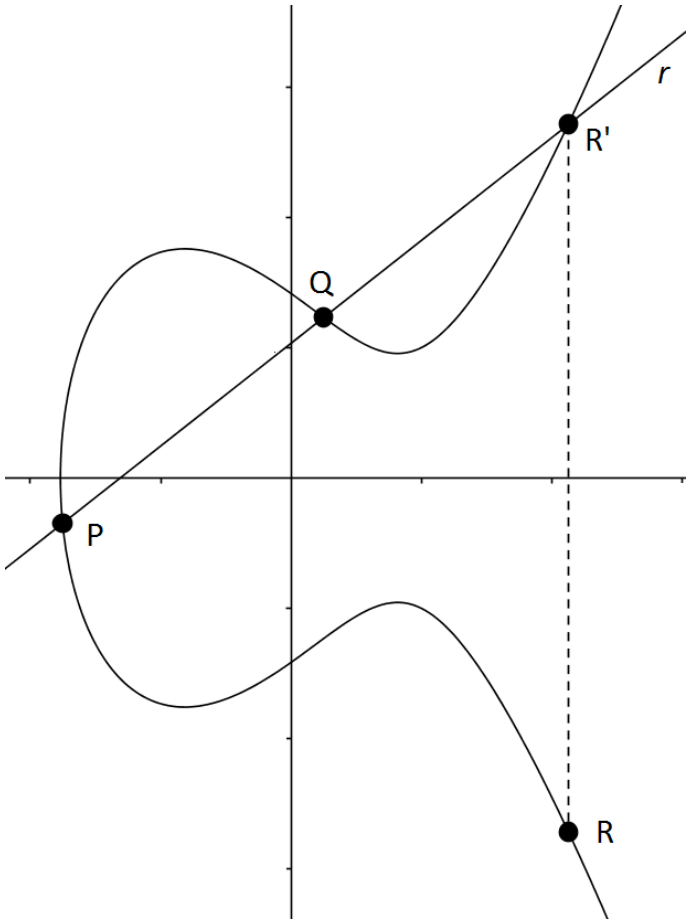

Figura 4.3: Soma de dois pontos em uma curva $E(\mathbb{R}) : R = P + Q$

Agora vamos definir a soma $P + P$, para isso tracemos a reta tangente ao ponto P, de tal modo que a reta tangente em P intersecta a curva em um segundo ponto R' e obtemos a reflexão R em relação ao eixo horizontal, ou seja $P + P = R$. Podemos representar a soma de $P + P$ por $2P$. Esse caso é ilustrado na Figura 4.4.

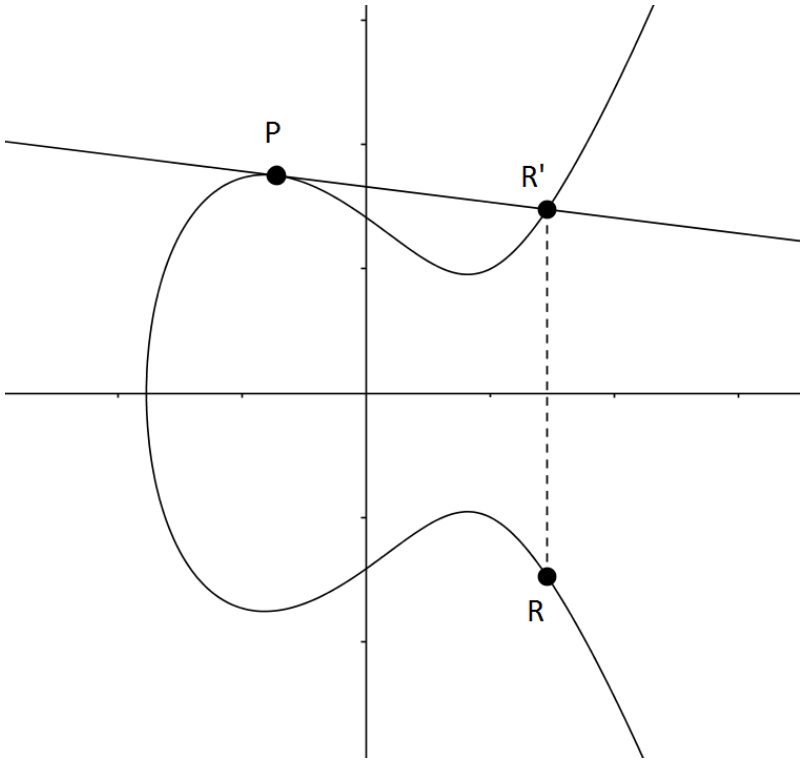

Figura 4.4: $R = P + P$ ou $R = 2P$

Um caso particular é disposto se tivermos $P = (x, 0)$, pois, neste caso, a reta tangente à curva no ponto P será vertical e não interceptará a curva em um outro ponto. Neste caso teremos:

$$P + P = 2P = \infty.$$

Veremos agora a soma de dois pontos utilizando a soma algébrica. Para tal iremos trabalhar com as coordenadas dos pontos em uma curva elíptica.

Seja $P = (x_p, y_p)$ e $Q = (x_q, y_q)$ dois pontos em uma curva elíptica Ω de equação $y^2 = x^3 + ax + b$, com $4a^3 + 27b^2 \neq 0$ e $P \neq \infty$ e $Q \neq \infty$, vamos analisar o caso $P \neq Q$. Seja r a reta que passa pelos pontos P e Q, que intersecta a curva Ω em um terceiro ponto que chamaremos de $R^{'} = (x_r^{'}, y_r^{'})$ e agora chamaremos de R a reflexão de $R^{'}$ com respeito ao eixo horizontal. Assim, pela fórmula da inclinação da reta, conclui-se que a inclinação da reta r é:

$$m = \frac{y_q - y_p}{x_q - x_p},$$

com $x_p \neq x_q$.

Logo a equação da reta r é:

$$y = m(x - x_p) + y_p$$

pois r passa pelo ponto P. Para obter as interseções entre a reta r e a curva Ω iremos substituir a equação da reta na equação da curva, veja:

$$(m(x - x_p) + y_p)^2 = x^3 + ax + b$$

$$\Longrightarrow m^2x^2 - 2m^2x_px + m^2x_p^2 + 2my_px - 2mx_py_p + y_p^2 = x^3 + ax + b$$

$$x^3 - m^2x^2 + (a + 2m^2x_p - 2my_p)x + (b - m^2x_p^2 + 2mx_py_p - y_p^2) = 0.$$

Tomando $a = -m^2, b = a + 2m^2x_p - 2my_p$ e $c = b - m^2x_p^2 + 2mx_py_p - y_p^2$

teremos:

$$x^3 + ax^2 + bx + c = 0.$$

Sabemos que P, Q e $R^{'}$ são as interseções da reta r com a curva Ω, então x_p, x_q e $x_r^{'}$ são as raízes da equação. Aplicando as Relações de Girard, temos que a soma das raízes é:

$$-a = x_p + x_q + x_r^{'}$$

Como $a = -m^2$ temos que :

$$m^2 = x_p + x_q + x_r^{'};$$

$$x_r^{'} = m^2 - x_p - x_q. \tag{4.1.1}$$

Como $R^{'} \in r$ podemos substituir suas coordenadas na equação da reta r, assim:

$$y^{'} = m(x_r^{'} - x_p) + y_p. \tag{4.1.2}$$

Como $R = P + Q$, $R = (x_r, y_r)$ é a reflexão de $R^{'}$ em relação ao eixo horizontal, assim $x_r = x_r^{'}$ e $y_r = -y_r^{'}$ substituindo nas equações (4.1.1) e (4.1.2) temos :

$$x_r = m^2 - x_p - x_q$$

e

$$y_r = m(x_p - x_r) - y_p.$$

Vamos analisar o caso que $P = Q$, nesse caso temos que a reta r é tangente à curva no ponto P. Assim, a inclinação da reta será a derivada no ponto P em relação a x. Usando derivação implícita, podemos concluir que:

$$m = \frac{3x_p^2 + a}{2y_p},$$

com $y_p \neq 0$, pois caso contrário a reta seria vertical e teríamos $P + P = \infty$. Logo, a reta r que passa por P com inclinação m tem a mesma forma da equação $y = m(x - x_p) + y_p$. Observe que se realizarmos a interseção desta reta com a curva Ω, obteremos a equação $x^3 + ax^2 + bx + c = 0$, porém agora as raízes não são todas distintas, pois x_p é uma raiz dupla. Assim, aplicando as Relações de Girard, temos que:

$$m^2 = x_p + x_p + x_r^{'};$$

$$x_r = x_r^{'} = m^2 - 2x_p.$$

Agora, para determinar y_r seguimos o mesmo procedimento para o caso $P \neq Q$ e temos

$$y_r = m(x_p - x_r) - y_p.$$

O caso em que $P = \infty$, teremos $x_r = x_p$ e $y_r = y_p$ e no caso $Q = \infty$, teremos $x_r = x_q$ e $y_r = y_q$, pois ∞ é o elemento neutro da operação.

Podemos, agora, padronizar a definição de soma entre dois pontos de uma curva elíptica em termos algébricos.

Definição 4.2. *(Soma de dois pontos de uma curva elíptica em termos algébricos) Seja Ω uma curva elíptica de equação $y^2 = x^3 + ax + b$, com $4a^3 + 27b^2 \neq 0$ e sejam $P = (x_p, y_p), Q = (x_q, y_q)$ e $R = (x_r, y_r)$ pontos da curva Ω tais que $R = P + Q$.*

- *Se $P = \infty$, então $R = Q$;*
- *Se $Q = \infty$, então $R = P$;*
- *Se $x_p = x_q$ e $y_p = -y_q$ então $R = \infty$*

caso contrário, defina

$$m = \begin{cases} \dfrac{y_q - y_p}{x_q - x_p}, & \text{se } P \neq Q; \\ \\ \dfrac{3x_p^2 + a}{2y_p}, & \text{se } P = Q. \end{cases}$$

Então:

$$x_r = \begin{cases} m^2 - x_p - x_q, & \text{se } P \neq Q; \\ \\ m^2 - 2x_p, & \text{se } P = Q. \end{cases}$$

e

$$y_r = m(x_p - x_r) - y_p$$

Definição 4.3. *Um grupo $(G, *)$ é um conjunto G com uma operação binária $*$ definida sobre G, de tal forma que as seguintes propriedades sejam válidas:*

- *A operação * é associativa, isto é, $\forall a, b, c \in G$ temos $a * (b * c) = (a * b) * c$*
- *Existe um elemento $e \in G$, chamado elemento neutro, tal que $\forall a \in G$ temos $a * e = e * a = a$.*
- *Para cada elemento $a \in G$ existe um elemento $a^{-1} \in G$, chamado elemento inverso, tal que $a * a^{-1} = a^{-1} * a = e$.*

Se a operação $*$ for comutativa, o grupo é chamado grupo comutativo ou grupo abeliano.

Proposição 4.4. *$(E(\mathbb{K}), +)$, onde $+$ é a operação de soma entre dois pontos de $\mathbb{K}$ é um grupo abeliano.*

Demonstração: Vejamos se $E(\mathbb{K})$ com a operação de soma entre dois pontos goza das propriedades de grupo abeliano:

P1: Associatividade

A demonstração pode ser encontrada em [9].

P2: Existência do Elemento Neutro

Sabemos que o ponto ∞ é o elemento neutro da soma entre dois pontos de uma curva elíptica e para qualquer $P \in E(\mathbb{K})$, temos $P + \infty = \infty + P = P$, logo existe elemento neutro.

P3: Existência do Elemento Inverso

Seja P um ponto qualquer da curva e o ponto $-P$ a reflexão do ponto P em relação ao eixo horizontal. Como a reta que passa por P e $-P$ é vertical, $P+(-P) = (-P) + P = \infty$.

P4: Comutatividade

A comutatividade segue do fato de que dados dois pontos P e Q da curva, a reta que passa por P e Q é a mesma que passa por Q e P, portanto, a interseção de ambas as retas com a curva é o mesmo ponto, logo, $P + Q = Q + P$.

Portanto $(E(\mathbb{K}), +)$ é um grupo abeliano.

□

A operação de soma é válida para qualquer corpo K, assim podemos trabalhar com curvas sobre corpos finitos. Trabalharemos com curvas sobre o corpo $\mathbb{Z}p$.

4.2 Curvas elípticas sobre o corpo $\mathbb{Z}_p$

Definição 4.5. *Uma curva elíptica sobre o corpo $\mathbb{Z}_p$, é o conjunto de pontos (x, y) com $x, y \in \mathbb{Z}_p$, tais que $y^2 = x^3 + ax + b$, com $a, b \in \mathbb{Z}_p$ e $4a^3 + 27b^2 \not\equiv 0$ mod p incluindo o ponto no infinito ∞.*

A curva $\mathbb{Z}_p$ possui um número finito de pontos, pois existem p possibilidades para a coordenada x e, para cada valor de x, existem dois valores possíveis para y. Assim, acrescentando o ponto infinito, uma curva no ponto $\mathbb{Z}_p$, terá, no máximo, $2p + 1$ pontos.

A curva E($\mathbb{K}$) é um conjunto finito de pontos. No exemplo abaixo iremos determinar todos os pontos de uma equação cúbica.

Exemplo 4.6. *Determine todos os pontos da curva $E(\mathbb{Z}_{11})$ de equação $y^2 = x^3 - x + 3$.*

Para descobrirmos se um ponto pertence à curva, tomamos cada valor de x, substituímos em $(x^3 - x + 3)$ mod 11 e averiguamos se este resultado é o quadrado módulo 11 de algum y. A tabela abaixo apresenta todos os valores possíveis de x e y.

y	y^2 *mod 11*	x	$x^3 - x + 3$ *mod 11*
0	0	0	3
1	1	1	3
2	4	2	9
3	9	3	5
4	5	4	8
5	3	5	2
6	3	6	4
7	5	7	9
8	9	8	1
9	4	9	8
10	1	10	3

Na tabela podemos observar, por exemplo, que para $x = 3$*, temos* $x^3 - x + 3 \equiv 5 \ mod\ 11$*, que por sua vez é quadrado módulo* 11 *de* $y = 4$ *e* $y = 7$*. Assim, os pontos* $(3, 4)$ *e* $(3, 7)$ *pertencem à curva. Note que para* $x = 5$ *temos* $x^3 - x + 3 \equiv 2 \ mod\ 11$*, mas não há nenhum valor de* y *cujo quadrado seja congruente a* 2 *módulo* 11*, ou seja, nenhum ponto da curva tem coordenada* $x = 5$*. Logo, os pontos da curva são:* $(0, 5), (0, 6), (1, 5), (1, 6), (2, 3), (2, 8), (3, 3), (3, 7), (6, 2), (6, 9), (7, 3), (7, 8), (8, 1), (8, 10), (10, 5)$ *e* $(10, 6)$.

Podemos observar que quanto maior o número primo p, mais inacessível se torna determinar todos os pontos de $E(\mathbb{Z}_p)$.

Na curva $E(\mathbb{Z}_p)$, queremos realizar a soma entre dois pontos na forma algébrica. Vejamos o exemplo abaixo:

Exemplo 4.7. *Seja a curva* $E(\mathbb{Z}_{11})$ *de equação* $y^2 = x^3 - x + 3$ *e os pontos* $P = (1, 5)$ *e* $Q = (2, 8)$ *pertencentes à curva. Calcule as coordenadas do ponto* $R = P + Q$*.*

Solução:

Como $P \neq Q$ *e* $x_p \neq x_q$*,*

$$m = \frac{y_q - y_p}{x_q - x_p} = 3.$$

Estamos trabalhando em $\mathbb{Z}_{11}$*, isto significa que* m *é o inteiro tal que* $1m \equiv 3 \ mod\ 11$*, logo,* $m = 3$*, pois* $1.3 = 3 \equiv 3 \ mod\ 11$*.*

Calculando a coordenada x_r*:*

$$x_r = m^2 - x_p - x_q$$

$$x_r = (3)^2 - 1 - 2$$

$$x_r = 6 \ mod\ 11.$$

Para y_r*:*

$$y_r = m(x_p - x_r) - y_p$$

$$y_r = 3(1 - 6) - 5$$

$$y_r = -20 \equiv -9 \equiv 2 \ mod\ 11.$$

Logo, $R = (6, 2)$ *e, pelo exemplo anterior,* $R \in \mathbb{Z}_{11}$.

4.3 Logaritmo discreto elíptico

Já vimos que se realizarmos a soma $P + P$ temos como resultado $2P$, que é múltiplo de P. Realizando o mesmo procedimento e somando P novamente, teremos $2P + P$ e o seu resultado será $3P$, fazendo esse procedimento n vezes, com $n \in \mathbb{N}$, temos:

$$P + P + P + \cdots + P = nP$$

Assim, dado um ponto $P \in E(\mathbb{Z}_p)$, podemos determinar os múltiplos $2P, 3P, \cdots, nP$ deste ponto P.

Exemplo 4.8. *Considere a curva* $E(\mathbb{Z}_{13})$ *de equação* $y^2 = x^3 + 2x - 1$. *Verifique se o ponto* $P = (5, 2)$ *pertence à curva e, em caso positivo, determine seus múltiplos.*

Solução: Encontrando os pontos da curva, que são: $(0, 5), (0, 8), (5, 2), (5, 11), (11, 0)$, $(12, 3)$ *e* $(12, 10)$. *Temos que* $P \in E(\mathbb{Z}_{13})$.

Iremos, agora, determinar os múltiplos de P *pela definição da soma algébrica.*

$$2P = P + P = (5, 2) + (5, 2) = (12, 3);$$

$$3P = 2P + P = (12, 3) + (5, 2) = (0, 8);$$

$$4P = 3P + P = (0, 8) + (5, 2) = (11, 0);$$

$$5P = 4P + P = (11, 0) + (5, 2) = (0, 5);$$

$$6P = 5P + P = (0, 5) + (5, 2) = (12, 10);$$

$$7P = 6P + P = (12, 10) + (5, 2) = (5, 11);$$

$$8P = 7P + P = (5, 11) + (5, 2) = \infty.$$

Observe que estes são os únicos múltiplos de P, pois como $8P = \infty$, a partir de $9P$ os resultados seriam repetidos.

Observe que, no exemplo anterior, todos os pontos da curva são múltiplos de $P = (5, 2)$, como $E(\mathbb{Z}_{13})$ com a operação de adição entre dois pontos é um grupo abeliano, dizemos que P é um gerador do grupo.

Podemos reescrever o Problema do Logaritmo Discreto à operação de soma entre dois pontos de uma curva sobre $\mathbb{Z}_p$. Considere um ponto $P \in E(\mathbb{Z}_p)$ tal que P seja um gerador de $E(\mathbb{Z}_p)$. Assim, para cada $Q \in E(\mathbb{Z}_p)$, existe $n \in (\mathbb{Z}_p)$ tal que

$$Q = nP$$

Onde n é o Logaritmo Discreto Elíptico de Q em relação a P, representado por $n = \log_P(Q)$. O Problema do Logaritmo Discreto Elíptico baseia-se em determinar n para cada ponto Q.

4.4 Criptografia com Curvas Elípticas

O referencial teórico empregado nesta seção pode ser averiguado nas obras de [8], [10] e [11].

4.4.1 Protocolo Diffie-Hellman aplicado a curvas elípticas sobre $\mathbb{Z}_p$

Vamos supor que duas pessoas, Maria e João desejam criar e compartilhar uma chave de codificação segura. Neste protocolo, além do número primo p e do gerador P, a equação da curva $E(\mathbb{Z}_p)$ é pública, pois Maria e João precisam calcular os pontos usando a mesma curva. Abaixo está descrito a metodologia do Protocolo Diffie-Hellman :

- Maria e João escolhem um primo p, uma curva $E(\mathbb{Z}_p)$ de equação $y^2 = x^3 + Ax + B$ com $\triangle = 4A^3 + 27B^2 \neq 0$, e um ponto $P \in E(\mathbb{Z}_p)$ gerador do grupo.
- Maria escolhe um inteiro $n_A \in \mathbb{Z}_p$, mantém secreto, e calcula $Q_A = n_A P$ e envia Q_A para João.
- João escolhe um inteiro n_B, mantém secreto, calcula $Q_B = n_B P$ e envia Q_B para Maria.
- Maria calcula $R_A = n_A Q_B$, que equivale a

$$R_A = n_A(n_B P) = (n_A n_B)P.$$

- João calcula $R_B = n_B Q_A$, que equivale a

$$R_B = n_B(n_A P) = (n_A n_B)P.$$

- Logo a chave secreta é $R_{AB} = R_A = R_B$.

Podemos observar que o método para criar e compartilhar a chave secreta é o mesmo. Logo, a comunicação pode ser realizada por um criptossistema qualquer. Caso um terceiro consiga capturar a comunicação, deverá calcular o logaritmo discreto elíptico de Q_A e Q_B para alcançar os dados iniciais.

Vejamos um exemplo:

Exemplo 4.9. *Considere a curva* $E(\mathbb{Z}_{11})$ *de equação* $y^2 = x^3 - x + 3$ *e o ponto* $P = (1, 5)$ *gerador de* $E(\mathbb{Z}_{11})$.

1. *Suponhamos que Maria escolha* $n_A = 3$, *e calcule* $Q_A = n_A P$, *ou seja,*

$$P = (1, 5)$$

$$2P = (2, 8)$$

$$3P = (6, 2) = Q_A$$

   e envia Q_A *para João.*

2. *Suponhamos que João escolha* $n_B = 2$, *e calcule* $Q_B = n_B P$, *ou seja,*

$$P = (1, 5)$$

$$2P = (2, 8)$$

   e envia Q_B *para Maria.*

3. *Maria então calcula* $R_A = n_A Q_B$, *ou seja,*

$$R_A = 3.(2, 8) = (3, 4)$$

4. *João calcula* $R_B = n_B Q_A$.

   Temos:

$$R_B = 2.(6, 2) = (3, 4)$$

Logo a chave secreta é $R_{AB} = R_A = R_B = (3, 4)$.

4.4.2 Criptossistema ElGamal

Iremos exemplificar o criptossistema de chave pública ElGamal utilizando, novamente, o caso Maria e João.

Mais uma vez, o primo p, a curva $E(\mathbb{Z}_p)$ da equação $y^2 = x^3 + ax + b$, com $4a^3 + 27b^2 \neq 0$, e o ponto $p \in E(\mathbb{Z}_p)$, gerador do grupo, são abertos para o público. Para iniciar o processo de encriptação João, que irá enviar uma mensagem a Maria, deve transformar a mensagem, que chamaremos de M, em um ponto $P_M \in E(\mathbb{Z}_p)$. Essa transformação pode ser realizada de várias maneiras, por exemplo, converter a mensagem por um inteiro utilizando a Tabela 4.1, onde cada letra do alfabeto, a partir de A, recebe um valor numérico iniciado em 1.

Tabela 4.1: Tabela de conversão ElGamal

Letra	Valor	Letra	Valor	Letra	Valor
A	01	J	10	S	19
B	02	K	11	T	20
C	03	L	12	U	21
D	04	M	13	V	22
E	05	N	14	W	23
F	06	O	15	X	24
G	07	P	16	Y	25
H	08	Q	17	Z	26
I	09	R	18		

Fonte: A autora.

Feito isso, separamos esse inteiro em duas coordenadas de um ponto, de maneira que este ponto pertença à curva $E(\mathbb{Z}_p)$. Caso o ponto gerado não pertença à curva, habitualmente acrescenta-se zero, ou outro algarismo ajustado entre as partes, no caso João e Maria, até que as coordenadas encontradas formem um ponto de $E(\mathbb{Z}_p)$.

Realizada esta transformação podemos iniciar a codificação.

Abaixo está descrito a metodologia do Criptossistema ElGamal:

1. Maria escolhe um inteiro secreto $n_A \in \mathbb{Z}_p$, calcula $Q_A = n_A P$ e envia Q_A para João.

2. João escolhe um inteiro aleatório k e calcula

$$R = kP \text{ e } S = P_M + kQ_A$$

3. João envia para Maria o par de pontos (R, S).

Para Maria decifrar a mensagem, basta calcular $S - n_A R$:

$$S - n_A R = P_M + kQ_A - n_A.kP = P_M + k.n_A P - k.n_A P = P_M.$$

Vejamos um exemplo:

Exemplo 4.10. *Considere a curva $E(\mathbb{Z}_{11})$ de equação $y^2 = x^3 - x + 3$ e o ponto $P = (1, 5)$ gerador de $E(\mathbb{Z}_{11})$ com a operação de soma entre dois pontos. Transforme a mensagem M em um ponto P_M da curva.*

Utilizando a Tabela 4.1 temos que a mensagem M = FI, em termos numéricos, corresponde ao inteiro 0609*, pois F=*06 *e I=*09*. Desmembrando este inteiro em duas coordenadas, encontramos o ponto $(06, 09) = (6, 9)$, vamos verificar se este ponto pertence a curva:*

$$y^2 = 9^2 = 81 \equiv 4 \ mod\ 11$$

$$x^3 - x + 3 = (6)^3 - 6 + 3 \equiv 216 - 6 + 3 = 213 \equiv 4 \ mod\ 11$$

Logo, a mensagem M é transformada no ponto $P_M = (6, 9)$.

Exemplo 4.11. *Agora, vamos supor, que João deseja enviar a mensagem M para Maria empregando o primo, a curva e o ponto gerador do exemplo anterior. Faça a codificação e decodificação da mensagem M utilizando o criptossistema ElGamal.*

Solução:

Usando os dados do exemplo anterior temos que $P_M = (6, 9)$*, Vejamos os passos do ElGamal:*

1. *Suponhamos que Maria escolha* $nA = 3$*. Temos:*

$$P = (1, 5)$$

$$2P = (2, 8)$$

$$3P = (6, 2) = Q_A$$

e envia para João.

2. *Suponhamos que João escolha* $k = 2$*, temos:*

$$R = kP = 2(1, 5) = (2, 8)$$

e

$$S = P_M = (6, 9) + KQ_A = (6, 9) + 2(6, 2) = (6, 9) + (3, 4) = (6, 2).$$

3. *João envia para Maria p par de pontos* (R, S)

Para decodificar a mensagem, basta Maria calcular

$$S - n_A R = (6, 2) - 3(2, 8) = (6, 2) - (3, 4) = (6, 2) + (3, 4 = (6, 2) + (3, 7) = (6, 9) = P_M.$$

Assim, Maria consegue ler a mensagem.

4.4.3 Vantagens e Desvantagens

O referencial teórico empregado nesta seção é averiguado na obra de [10], [11] e [8].

A Criptografia de Curvas Elípticas está grandemente reconhecida como o algoritmo mais forte para um dado comprimento de chaves, ela utiliza um período parcialmente curto de criptografia chave (valor mantido no algoritmo de criptografia para decodificar uma mensagem criptografada). Esta chave de curto período, além de carecer menos poder computacional é mais rápida do que os outros de criptografia de primeira geração com algoritmos de chave pública. As vantagens da Criptografia de Curvas Elípticas são essencialmente significativas em dispositivos sem fio, onde o poder de computação, memória e vida útil da bateria é limitada.

Uma das desvantagens da Criptografia de Curvas Elípticas é que sua execução é mais complexa e difícil, o que aumenta a probabilidade de erros de implementação. Além disso, o tamanho da mensagem criptografada é significativamente maior comparado ao RSA, por exemplo.

CAPÍTULO 5

CONSIDERAÇÕES FINAIS

No desenvolvimento deste estudo vimos o método RSA e a criptografia com curvas elípticas que vem se destacando ultimamente, haja visto sua utilização em criptomoedas. Porém, temos a certeza que os dois métodos padecem de um problema: ambos tem um prazo de validade. Pois assim como os métodos criptográficos se desenvolvem, o desenvolvimento para a criação de computadores melhores, por exemplo a computação quântica, para quebrá-los também aumenta.

Infelizmente, não conseguimos atingir o objetivo de desvendar a criptografia que está por trás do Bitcoin, por falta de materiais adequados. Porém, pretende-se, com este trabalho, contribuir para o enriquecimento de bibliografia sobre o tema, que ainda é limitada, sistematizando e compilando em um único texto muitas informações e exibir o algoritmo que está por trás dos processos. Assim, continuações naturais deste trabalho podem aparecer, seja para seguir desvendando os algoritmos das criptomoedas, seja para traduzir temas complexos relacionados a criptografia para linguagem cotidiana com o intuito de motivar os alunos a estudar matemática.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] D. D. Costa, *A matemática e os códigos secretos : uma introdução à criptografia / Claudio Saldan.* Maringá, PR, 2014.

[2] S. Coutinho, *Números Inteiros e Criptografia RSA.* Rio de Janeiro, RJ : IMPA, 2009.

[3] K. A. B. C. Carvalho, *A Criptografia*

no Ensino da Matemática: aplicações para a Educação básica, Dissertação Mestrado Profissional em Matemática - PROFMAT/UEMA. Rio de Janeiro, 2018.

[4] A. HEFEZ, *Aritmética.* Rio de Janeiro, 2014.

[5] E. G. Andrade, *Criptografia com curvas elipticas. 2016. 78f. Dissertação (Mestrado Profissional em Matemática - PROFMAT)-Universidade Federal do Pará Instituto de Ciências Exatas e Naturais.* Belém, 2016.

[6] J. G. Oliveira, *Curvas Elípticas sobre Corpos Finitos e Criptografia de Chave Pública. 2009. 12f. Universidade Federal do Mato Grosso do Sul.* Campo Grande - MS, novembro 2009.

[7] S. S. J. Correia, *Criptografia via curvas elípticas. 2013. 87f. Dissertação (Mestrado Profissional em Matemática - PROFMAT)- Universidade Federal do Estado do Rio de Janeiro - UNIRIO.* Rio de Janeiro, 2013.

[8] F. B. Lara, P. C. S; Oliveira, *Curvas Elípticas: Aplicação em Criptografia Assimétrica.10f. 1Laboratório Nacional de Computação Científica – LNCC.* Petrópolis, RJ.

[9] L. C. WASHINGTON, *Elliptic Curves: number theory and criptography,.* Boca Raton: Chapman and Hall, 2nd edition ed., 2008.

[10] *Quais são as vantagens e desvantagens de Elliptic Curve Cryptography para segurança sem fio. Disponível em: <http://ptcomputador.com/Networking/wireless-networking/81737.html>*, Acesso em: 17 maio. 2019.

[11] *Segurança Lógica de Software. Disponível em: <http://segurancalogica01.blogspot.com/2008/04/criptografia-com-o-uso-de-curvas.html>*, Acesso em: 17 maio. 2019.

[12] G. Domingues, H. H; Iezzi, *Álgebra moderna.* São Paulo, SP : Atual, 4. ed. reform. 5. tir ed., 2011.

[13] E. L. e. a. Lima, *A matemática do ensino médio.* Rio de Janeiro, RJ : Sociedade Brasileira de Matemática, 10. ed. redigitada e rev ed., 2012.

[14] A. C. M. Neto, *Tópicos de matemática elementar.* Rio de Janeiro, RJ : SBM, 2. ed. ed., 2013.

[15] I. N. Herstein, *Tópicos de álgebra / Israel Nathan Herstein ; tradução de Adalberto P. Bergamasco e L. H. Jacy Monteiro.* São Paulo, SP : Polígono,, 1970.

[16] E. L. e. a. Lima, *Temas e problemas.* Rio de Janeiro, RJ : SBM, 3. ed. ed., 2003.