SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

EDISON GARRETA DE ANDRADE

CRIPTOGRAFIA COM CURVAS ELÍPTICAS

BELÉM
2016

SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

EDISON GARRETA DE ANDRADE

CRIPTOGRAFIA COM CURVAS ELÍPTICAS

Dissertação apresentada como requisito parcial para obtenção do grau de mestre em matemática pelo Programa de Mestrado Profissional em Matemática (PROFMAT) da Universidade Federal do Pará

Orientador: Prof[a]. Dr[a]. Irene Castro Pereira

BELÉM
2016

Dados Internacionais de Catalogação-na-Publicação (CIP)
Sistema de Bibliotecas da UFPA

Andrade, Edison Garreta de, 1986-
Criptografia com curvas elípticas / Edison Garreta de Andrade. - 2016.

Orientadora: Irene Castro Pereira.
Dissertação (Mestrado) - Universidade Federal do Pará, Instituto de Ciências Exatas e Naturais, Programa de Pós-Graduação em Matemática (Mestrado Profissional), Belém, 2016.

1. Criptografia. 2. Curvas elípticas. 3. Logarítimos. I. Título.

CDD 22. ed. 005.82

Edison Garreta de Andrade

CRIPTOGRAFIA COM CURVAS ELÍPTICAS

Dissertação submetida à Coordenação Acadêmica do Programa de Mestrado Profissional em Matemática em Rede Nacional na Universidade Federal do Pará, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovada em 18 de Fevereiro de 2016, por

BANCA EXAMINADORA

Profª. Drª. Irene Castro Pereira (Orientadora)
UNIVERSIDADE FEDERAL DO PARÁ

Profª. Drª. Maria de Nazaré Carvalho Bezerra
UNIVERSIDADE FEDERAL DO PARÁ

Prof. Dr. Pedro Silvestre da Silva Campos
UNIVERSIDADE FEDERAL RURAL DA AMAZÔNIA

BELÉM
Fevereiro de 2016

À minha família, por sempre acreditar em mim.

AGRADECIMENTOS

Ao grande Pai celestial, por ser tão bondoso comigo desde sempre.

A meus pais, pelo apoio incondicional, desde que decidi sair de Igarapé-Açu para Belém pra fazer a graduação.

A toda minha família, em especial a minha irmã Kleide, por ser uma inspiração desde a infância e indiretamente me levar para a docência. Jamais conseguirei retribuir todos os ensinamentos recebidos.

Aos amigos espirituais, pelas valorosas contribuições nos momentos difíceis e pela inspiração quanto ao tema.

A Paulo Sérgio, pelo apoio, compreensão e companheirismo ao longo do curso.

Aos amigos e colegas de trabalho, em especial as amigas Emília e Cris Brasil, pelas cobranças e motivações.

A meus alunos do ensino fundamental da Escola Municipal Francisco Espinheiro Gomes, do município de Castanhal – Pará, pela curiosidade em saber porque eu ainda continuo estudando e pelo constante interesse em meu trabalho, mesmo não compreendendo-o.

A meus amigos da época do BNB, pela torcida e pelas energias positivas.

A Universidade Federal do Pará, ao Programa de Mestrado Profissional em Matemática – PROFMAT e a CAPES, pela oportunidade de aprimoramento.

Aos colegas de curso, em especial Jhon e Serginho, por se preocuparem mais comigo do que eu mesmo.

A todos os professores do curso.

A minha orientadora Professora Dr^{a}. Irene Castro Pereira, pela disponibilidade, pelos conselhos ao longo da realização deste trabalho e por me repassar parte de seu conhecimento.

"A felicidade não está na partida e nem na chegada, mas na travessia."

Guimarães Rosa

Resumo

Neste trabalho estudamos um criptossistema de chave pública que utiliza curvas elípticas a partir de uma adaptação do Problema do Logaritmo Discreto. Este sistema se utiliza da dificuldade de resolver o Problema do Logaritmo Discreto para garantir segurança à transmissão de dados, principalmente quando o mesmo é aplicado a curvas elípticas sobre corpos finitos. São apresentadas algumas sugestões de atividades para aplicação em turmas de ensino médio utilizando o tema deste trabalho como motivação.

Palavras-chave: criptografia, curvas elípticas, problema do logaritmo discreto.

Abstract

In this work we study a public-key cryptosystem that uses elliptic curves through an adaptation of the Discrete Logarithm Problem. This system makes use of the fact that it's not easy to solve the Discrete Logarithm Problem to guarantee security in data transmission, especially when applied to elliptic curves over finite fields. We show some activities to be applied to high school classes using the subject of this work as motivation.

Keywords: criptography, elliptic curves, discrete logarithm problem.

Sumário

INTRODUÇÃO

Neste trabalho abordamos um método de criptografia envolvendo curvas elípticas, inicialmente proposto por Koblitz e Miller. Criptografia é a arte de esconder a escrita, na tentativa de impedir que pessoas não autorizadas tenham acesso ao conteúdo de uma mensagem. Os algoritmos de criptografia podem ser classificados de acordo com a chave de encriptação: *criptografia de chave secreta ou simétrica* – quando apenas os sujeitos envolvidos na comunicação possuem conhecimento da chave – e *criptografia de chave pública* – quando a chave de encriptação é de conhecimento público.

Diversos algoritmos de criptografia já foram propostos até hoje, cada um com vantagens e desvantagens, como por exemplo: Cifra de César, Protocolo Diffie-Helman, RSA e Criptografia com Curvas Elípticas (ECC). Este último tem demonstrado ser mais eficiente do que o RSA quanto a espaço de memória utilizado e tempo de processamento, fornecendo relativamente o mesmo nível de segurança [9]. Entretanto, o RSA continua sendo o algoritmo mais utilizado devido a poucos estudos sobre ECC, até mesmo envolvendo suas possíveis vulnerabilidades.

No capítulo 1, abordamos conceitos essenciais para a compreensão deste trabalho, a saber, principais resultados da Teoria dos Números, alguns conceitos introdutórios de Álgebra Abstrata e noções básicas de Criptografia.

No capítulo 2, conceituamos logaritmo discreto e definimos o Problema do Logaritmo Discreto (PLD). Mostramos como a dificuldade de resolução do PLD contribui para a segurança da informação e apresentamos dois algoritmos criptográficos que utilizam diretamente o PLD como forma de garantir segurança: protocolo Diffie-Hellman e criptossistema

ElGamal.

No capítulo 3, definimos curvas elípticas a partir de uma modificação na equação de Weierstrass e a operação de soma sobre dois pontos de uma curva, tanto na forma geométrica quanto na forma algébrica. Esta operação é essencial para discretizar a curva, adaptando-a para uma estrutura sobre um corpo $\mathbb{Z}_p$.

No capítulo 4, adaptamos o PLD para a estrutura de curvas elípticas, deste modo podemos aplicar algoritmos de criptografia a esta estrutura.

No capítulo 5, sugerimos atividades para o ensino médio, com base no tema abordado neste trabalho, desde o uso de noções básicas de criptografia como recurso educacional, até uma simulação de um algoritmo criptográfico envolvendo curvas elípticas.

Capítulo 1

CONCEITOS ESSENCIAIS

Antes de discutir curvas elípticas e métodos de criptografia, vamos, inicialmente, revisar alguns resultados da Teoria dos Números, bem como a definição de grupo e conceitos de criptografia, essenciais para a compreensão deste trabalho.

1.1 Números Inteiros

O conjunto de todos os números inteiros é representado por $\mathbb{Z}$. Sejam $a, b, c \in \mathbb{Z}$, a soma e a multiplicação de dois inteiros quaisquer gozam das seguintes propriedades:

A1. Propriedade Associativa da Adição: $a + (b + c) = (a + b) + c$.

A2. Propriedade Comutativa da Adição: $a + b = b + a$.

A3. Existência do Elemento Neutro Aditivo: existe um único $0 \in \mathbb{Z}$ tal que $a + 0 = a$.

A4. Existência do Elemento Oposto Aditivo: para todo a existe um $-a$ tal que $a+(-a) = 0$.

M1. Propriedade Associativa da Multiplicação: $a(bc) = (ab)c$.

M2. Propriedade Comutativa da Multiplicação: $ab = ba$.

M3. Existência do Elemento Neutro da Multiplicação: existe um único $1 \in \mathbb{Z}$ tal que $1.a = a$.

M4. Propriedade Cancelativa da Multiplicação: se $ab = ac$ com $a \neq 0$, então $b = c$.

D1. Propriedade Distributiva: $a(b+c) = ab + ac$.

Definição 1.1.1. *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Dizemos que b divide a se existe um inteiro q tal que $a = bq$. Escrevemos*

$$b \mid a$$

Dizemos que b é um *divisor* de a. Caso não exista nenhum inteiro q tal que $a = bq$, diz-se que b não divide a e representa-se $b \nmid a$.

Definição 1.1.2 (Números Primos e Compostos)**.** *Um inteiro $a > 1$ é dito primo se os únicos divisores positivos de a são 1 e o próprio a. Dizemos que a é um número composto se a não é primo.*

Com estas definições, podemos enunciar um importante resultado da Teoria dos Números.

Teorema 1.1 (Teorema Fundamental da Aritmética)**.** *Todo número inteiro positivo maior que 1 pode ser escrito de maneira única como o produto de números primos, a menos da ordem dos fatores.*

A demonstração deste teorema pode ser consultada no anexo A.

□

Teorema 1.2 (Divisão Inteira)**.** *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Existem inteiros q e r únicos tais que $a = bq + r$, com $0 \leq r < |b|$.*

Demonstração:

Vejamos, primeiramente, o caso em que $b > 0$ e a qualquer.

Consideremos $a \geq 0$. Seja S o conjunto de todos os inteiros não negativos n tais que $a - bn$ é não negativo. Deste modo, $0 \in S$, pois $a - b.0 = a \geq 0$, logo, $S \neq \emptyset$. Temos também que S é limitado, pois para todo $n > a/b$, temos $a - bn < 0$. Seja q o elemento máximo de S. Tomando $r = a - bq$, temos $r < b$, caso contrário $q + 1$ também estaria em S. Logo, existem inteiros q e r tais que $a = bq + r$, com $0 \leq r < b$.

Para o caso $a < 0$, podemos, pelo resultado acima, encontrar q' e r' tais que

$$|a| = bq' + r' \text{ e } 0 \leq r' < b$$

Como $a < 0$, temos $|a| = -a$

Se $r' = 0$:

$$-|a| = -(bq' + 0)$$

$$a = b(-q') + 0$$

logo, $q = -q'$ e $r = 0$ satisfazem as condições.

Se $r' > 0$:

$$-|a| = -(bq' + r')$$

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

logo, $q = -q'$ e $r = -r'$ satisfazem as condições

Vejamos, agora, o caso $b < 0$. Pela parte anterior, para qualquer inteiro a, conseguimos encontrar q' e r' tais que

$$a = |b|q' + r' \text{ e } 0 \leq r' < |b|$$

Como $b < 0$, temos que $|b| = -b$, logo,

$$a = |b|q' + r' = (-b)q' + r' = b(-q') + r'$$

.

Os inteiros $q = -q'$ e $r = r'$ satisfazem as condições do enunciado do teorema. Deste modo, sempre é possível encontrar q e r nas condições descritas.

Vejamos, agora, a unicidade. Sejam a e b tais

$$a = bq + r$$

e

$$a = bq' + r'$$

Temos que

$$bq + r = bq' + r'$$

$$(q - q')b = r' - r$$

Suponhamos que $r' \geq r$. Como $r' < |b|$ e $r < |b|$, concluímos que $r' - r < |b|$, logo:

$$(q - q')b < |b|$$

$$0 \leq |q - q'|.|b| < |b|$$

aplicando a propriedade cancelativa da multiplicação, obtemos:

$$0 \leq |q - q'| < 1$$

Como q e q' são inteiros, conclui-se que $|q - q'| = 0$, logo, $q = q'$. Substituindo em $bq + r = bq' + r'$, encontramos $r = r'$. Portanto, os inteiros q e r são únicos.

□

Definição 1.1.3. *Sejam a e b inteiros, com $b \neq 0$, tais que $a = bq + r$, com q e r inteiros e $0 \leq r < |b|$. Os inteiro q e r são denominados, respectivamente, quociente e resto da divisão de a por b.*

Definição 1.1.4 (Congruência)**.** *Seja $m \neq 0$ um inteiro fixo. Dois inteiros a e b são congruentes módulo m se m divide a diferença $a - b$, ou seja, $m \mid (a - b)$. Escrevemos*

$$a \equiv b \ (\mathrm{mod}\ m)$$

Proposição 1.1. *Seja $m \neq 0$ um inteiro fixo. Dois inteiros a e b são congruentes módulo m se, e somente se, o resto da divisão de a por m é igual ao resto da divisão de b por m.*

Demonstração:

Sejam

$$a = mq_1 + r_1, \quad \text{com} \quad 0 \leq r_1 < |m|$$
$$b = mq_2 + r_2, \quad \text{com} \quad 0 \leq r_2 < |m|$$

Então:

$$a - b = m(q_1 - q_2) + (r_1 - r_2)$$

Logo,

$$m \mid (a - b), \text{ se e somente se } m \mid (r_1 - r_2)$$

Como $0 \leq |r_1 - r_2| < m$, temos que $m \mid |r_1 - r_2|$ se e somente se $|r_1 - r_2| = 0$, ou seja, se e somente se $r_1 = r_2$.

Logo, $a \equiv b \pmod{m}$ se e somente se $r_1 = r_2$.

□

Definição 1.1.5 (Sistema Completo de Resíduos)**.** *O conjunto dos inteiros* $\mathbb{Z}_m = \{r_1, r_2, \ldots, r_m\}$ *é um sistema completo de resíduos módulo* m *se:*

(i) $r_i \not\equiv r_j$ *módulo* m *para* $i \neq j$

(ii) $\forall n \in \mathbb{Z}$*, existe um* r_i *tal que* $n \equiv r_i \pmod{m}$

Alguns exemplos de sistemas completos de resíduos módulo 5 são:

$$\{0, 1, 2, 3, 4\}$$
$$\{5, 6, 7, 8, 9\}$$
$$\{31, 47, -1, 15, 23\}$$

Se p é primo, $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ é um sistema completo de resíduos. Isto é facilmente verificável, pois p é relativamente primo a qualquer inteiro positivo menor que p.

Teorema 1.3 (Pequeno Teorema de Fermat)**.** *Sejam* p *primo e* a *um inteiro. Se* $p \nmid a$*, então* $a^{p-1} \equiv 1 \pmod{p}$.

A demonstração deste teorema pode ser vista no anexo B.

□

Corolário 1.1. *Se* p *é um primo e* a *é um inteiro positivo, então* $a^p \equiv a \pmod{p}$.

Demonstração

Temos que analisar dois casos: se $p \mid a$ e se $p \nmid a$.

Se $p \mid a$, então

$$p \mid a(a^{p-1} - 1) \Leftrightarrow p \mid (a^p - a)$$

portanto, $a^p \equiv a \pmod{p}$.

Se $p \nmid a$, pelo teorema 1.3, $p \mid (a^{p-1} - 1)$ e, portanto, $p \mid a(a^{p-1} - 1) \Leftrightarrow p \mid (a^p - a)$

Logo, em ambos os casos, $a^p \equiv a \pmod{p}$.

□

Definição 1.1.6 (Função ϕ de Euler)**.** *Para cada inteiro $n \geq 1$ indicaremos por $\phi(n)$ o número de inteiros positivos, menores ou iguais a n, que são relativamente primos com n. A função assim definida chama-se função ϕ de Euler.*

Definição 1.1.7. *Sistema reduzido de resíduos módulo m é um conjunto com $\phi(m)$ inteiros $r_1, r_2, \ldots, r_{\phi(m)}$, tais que cada elemento do conjunto é relativamente primo com m e se $i \neq j$, então $r_i \not\equiv r_j \mod m$.*

Teorema 1.4. *Seja a um inteiro positivo tal que $\text{mdc}(a, m) = 1$. Se $r_1, r_2, \ldots, r_{\phi(m)}$ é um conjunto reduzido de resíduos módulo m, então $ar_1, ar_2, \ldots, ar_{\phi(m)}$ também o é.*

Ideia da Demonstração

Cada um dos $\phi(m)$ números é relativamente primo com m (pois cada fator comum de ar_i deveria dividir r_i e m). Além disso, cada par é incongruente. Para uma demonstração mais completa, ver [10].

□

Teorema 1.5 (Teorema de Euler)**.** *Sejam $a, m \in \mathbb{Z}$ com $m \geq 1$, tais que $\text{mdc}(a, m) = 1$, então*

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Para demonstração, ver anexo C

□

1.2 Grupos, Anéis e Corpos

Definição 1.2.1. *Um grupo $(G, *)$ é um conjunto G com uma operação binária $*$ definida sobre G, de tal forma que as seguintes propriedades sejam válidas:*

P1. *A operação $*$ é associativa, isto é, $\forall a, b, c \in G$ temos $a * (b * c) = (a * b) * c$.*

P2. *Existe um elemento $e \in G$, chamado elemento neutro, tal que $\forall a \in G$ temos $a * e = e * a = a$.*

P3. *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, ou seja, $\forall a, b \in G : a * b = b * a$, o grupo é chamado *grupo comutativo* ou *grupo abeliano*.

Definição 1.2.2. *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.

Um exemplo de grupo multiplicativo é $\mathbb{Z}_7^*$:

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

Se existe um elemento $g \in G$ tal que $\forall a \in G, \exists j \in \mathbb{Z}$ tal que $g^j = a$, dizemos que $(G, *)$ é um grupo *cíclico* e g é um *gerador* de $(G, *)$.

Por exemplo, 3 é um gerador de $\mathbb{Z}_7^*$, pois:

$$3^1 \equiv 3 \pmod 7$$
$$3^2 \equiv 2 \pmod 7$$
$$3^3 \equiv 6 \pmod 7$$
$$3^4 \equiv 4 \pmod 7$$
$$3^5 \equiv 5 \pmod 7$$
$$3^6 \equiv 1 \pmod 7$$

Definição 1.2.3. *Um conjunto não-vazio A é chamado anel se em A estão definidas duas operações $+$ e $*$, tais que, $\forall a, b \in A$, temos:*

- $a + b \in A$
- $a + b = b + a$

- $(a + b) + c = a + (b + c)$
- $\exists e \in A$ *tal que* $a + e = a$, $\forall a \in R$
- $\exists -a \in A$ *tal que* $a + (-a) = e$
- $a * b \in A$
- $a * (b * c) = (a * b) * c$
- $a * (b + c) = a * b + a * c$
- $(b + c) * a = b * a + c * a$

Se além de todas estas propriedades a operação $*$ for comutativa, ou seja, $a*b = b*a$, dizemos que R é um anel comutativo.

Definição 1.2.4. *Seja* $\mathbb{K}$ *um anel comutativo com unidade*[1]. *Se* $\forall x \in \mathbb{K}$, *com* $x \neq 0$, $\exists y \in \mathbb{K}$ *tal que* $x * y = y * x = 1$, *dizemos que* $\mathbb{K}$ *é um corpo.*

Segundo GONÇALVES [5], um corpo é um anel comutativo no qual cada elemento não nulo possui inverso multiplicativo.

Dizemos que um corpo é finito quando o mesmo possui uma quantidade finita de elementos.

Definição 1.2.5. *Seja* p *um número primo. O conjunto* $\mathbb{Z}_p$, *formado pelos inteiros não negativos menores que* p,

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p - 1\}$$

e para o qual estão definidas as operações de adição e multiplicação é um corpo finito.

1.3 Criptografia

Criptografia é a arte e ciência de cifrar a escrita, ou seja, torná-la ininteligível. Segundo TERADA [15], o objetivo principal da criptografia é "esconder informações sigilosas de qualquer pessoa desautorizada a lê-las, isto é, de qualquer pessoa que não conheça a

[1] isto é, existe elemento neutro para a operação $*$

chamada chave secreta de criptografia". De forma mais geral, STINSON [14] diz que a criptografia objetiva permitir a comunicação entre duas pessoas, por meio de um canal inseguro, de tal forma que uma terceira pessoa (um intruso) não consiga compreender a mensagem. O conteúdo da comunicação, que neste trabalho será referenciado como mensagem, pode ser um texto, dados numéricos, um arquivo, ou qualquer outro tipo de conteúdo.

Definição 1.3.1 (Chave de codificação)**.** *Chamamos de chave à informação necessária para cifrar e decifrar uma mensagem.*

No escopo deste trabalho, uma chave pode ser um inteiro ou uma n-upla de inteiros.

Para encriptar uma mensagem é necessário, primeiramente, que os sujeitos envolvidos entrem em acordo quanto ao sistema de criptografia, também chamado criptossistema, que empregarão.

Definição 1.3.2 (Criptossistema)**.** *Criptossistema é uma quíntupla* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *na qual*

1. $\mathcal{P}$ *é um conjunto finito de possíveis textos legíveis;*
2. $\mathcal{C}$ *é um conjunto finito de possíveis textos cifrados;*
3. $\mathcal{K}$ *é um conjunto finito com todas as possíveis chaves de codificação;*
4. $\mathcal{E}$ *é um conjunto com todas as regras de encriptação ou codificação de um texto legível;*
5. $\mathcal{D}$ *é um conjunto com todas as regras de decodificação de um texto cifrado.*

Ao escolher o criptossistema utilizado na encriptação da mensagem, já se determina como a mensagem será cifrada pelo remetente e quais procedimentos o destinatário deverá realizar para decodificar a mensagem cifrada recebida, podendo, desta forma, ler a mensagem original.
Empregando a notação da definição 1.3.2, temos que para cada chave $K \in \mathcal{K}$, existe uma regra ou função de codificação $E_K \in \mathcal{E}, E_K : \mathcal{P} \to \mathcal{C}$ e uma correspondente regra de decodificação $D_K \in \mathcal{D}, D_K : \mathcal{C} \to \mathcal{P}$ tais que

$$D_K(E_K(x)) = x$$

para qualquer $x \in \mathcal{P}$.[2]

Os criptossistemas são classificados de acordo com o tipo de chave utilizada, podendo a mesma ser secreta ou pública.

1.3.1 Criptografia de Chave Secreta

Quando um emissor deseja encriptar uma mensagem e enviá-la a um único receptor e pretende que somente este consiga decodificá-la, é intuitivo que se deseje compartilhar uma *chave secreta* K, ou seja, a chave utilizada pelo emissor para codificar a mensagem é a mesma utilizada pelo receptor para decodificá-la. Por este motivo, é também chamado de criptografia de chave simétrica ou compartilhada. É considerado pouco seguro, pois é necessário que a chave de codificação também seja compartilhada por um canal que é desejavelmente seguro, mas está sujeito a interceptação de intrusos. Deste modo, para que uma pessoa não autorizada decifrasse a mensagem, seria necessário apenas ter posse da chave utilizada e do texto cifrado, pois neste caso D_K é facilmente determinável a partir de E_K.

Para diminuir o risco de quebra de código, os criptossistemas de chave secreta costumam realizar permutações de blocos de textos da mensagem original, ou mesmo alterações na própria chave de encriptação para gerar subchaves. Alguns exemplos de sistemas de criptografia de chave secreta são: *Data Encryption Standard* (DES), *International Data Encryption Algorithm* (IDEA) e *Secur and Fast Encryption Routine* (SAFER K-64). Na seção 2.1 será visto um protocolo para melhorar a segurança no compartilhamento de chaves secretas.

1.3.2 Criptografia de Chave Pública

Para resolver o problema de enviar uma chave secreta sem que a mesma seja interceptada por intrusos (o que implicaria quebra de código), faz-se necessário um sistema no qual a mensagem original continue intacta mesmo que um estranho tenha conhecimento da chave empregada. Ou seja, deseja-se que caso E_K seja conhecido, seja difícil determinar D_K. Deste modo, E_K pode até mesmo ser divulgado, pois a dificuldade de computar D_K garante

[2] D_K é a função inversa de E_K

a segurança. Por este motivo este sistema é chamado de criptografia de chave pública.

Neste sistema, cada usuário possui um par de chaves (S, P), com $S, P \in \mathcal{K}$. S é sua chave secreta e P sua chave pública. Devido a chaves diferentes serem utilizadas durante o processo de codificação/decodificação, também chamamos este sistema de criptografia de chave assimétrica.

Alguns exemplos de sistema de criptografia de chave pública são: Algoritmo RSA, Algoritmo Rabin e Criptografia com Curvas Elípticas.

Capítulo 2

PROBLEMA DO LOGARITMO DISCRETO

Diversos sistemas de criptografia de chave pública são baseados na dificuldade de resolver o Problema do Logaritmo Discreto, entre eles o objeto de estudo deste trabalho, criptografia com curvas elípticas.

Sejam $(G, \times)$ um grupo multiplicativo e $\alpha, \beta \in G$. Pretendemos encontrar um inteiro x tal que

$$\alpha^x = \beta$$

O inteiro x denotado por $\log_\alpha \beta$ é chamado de logaritmo discreto de β.

De acordo com STINSON [14], determinar o logaritmo discreto em $\mathbb{Z}_p$ é considerado um problema intratável[1] quando p possui no mínimo 150 algarismos. Por este motivo, trataremos o logaritmo discreto limitado a $\mathbb{Z}_p$.

Seja p primo e seja $a \in \mathbb{Z}$ com $a \not\equiv 0 \pmod{p}$. Suponhamos que para cada inteiro b, com $b \not\equiv 0 \pmod{p}$, exista um inteiro x tal que

$$a^x \equiv b \ (\mod p)$$

O Problema do Logaritmo Discreto consiste em encontrar o inteiro x para cada b.

[1] "*Certos problemas computacionais são solúveis em princípio, mas as soluções requerem tanto tempo ou espaço que elas não podem ser usadas na prática. Tais problemas são chamados* ***intratáveis***". (SIPSER, 2007. pg 355)[12]

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

Demonstração:

Seja x uma solução para a congruência. Pelo teorema 1.3 (P.T.F.), temos que

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

Deste modo, temos:

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

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:

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

Logo, a congruência possui infinitas soluções inteiras.

□

Para evitar uma multiplicidade de soluções, restringiremos o expoente x ao corpo $\mathbb{Z}_p$.

Proposição 2.2. *Dado um inteiro fixo $a \neq 0$, o problema do logaritmo discreto $a^x \equiv b \pmod{p}$ possui solução em $\mathbb{Z}_p$ para qualquer $b \in \mathbb{Z}_p$, com $b \not\equiv 0 \pmod{p}$, se, e somente se, a é um gerador do grupo multiplicativo $\mathbb{Z}_p^*$.*

Demonstração:

Considere que $a^x \equiv b \pmod{p}$ 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 $a^x \equiv b \pmod{p}$, logo, a é um gerador de $\mathbb{Z}_p^*$.

Agora, considere 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 $a^x \equiv b \pmod{p}$, logo, o problema do logaritmo discreto possui solução.

□

Vejamos um exemplo.

Exemplo 2.1. *Calcular* $x = \log_7 9$ *em* $\mathbb{Z}_{11}$.

Solução:

Verificamos, primeiramente, que 7 é um gerador do grupo multiplicativo $\mathbb{Z}_{11}^*$. De fato, temos:

$$\begin{aligned} 7^1 &\equiv 7 \pmod{11} \\ 7^2 &\equiv 5 \pmod{11} \\ 7^3 &\equiv 2 \pmod{11} \\ 7^4 &\equiv 3 \pmod{11} \\ 7^5 &\equiv 10 \pmod{11} \\ 7^6 &\equiv 4 \pmod{11} \\ 7^7 &\equiv 6 \pmod{11} \\ 7^8 &\equiv 9 \pmod{11} \\ 7^9 &\equiv 8 \pmod{11} \\ 7^{10} &\equiv 1 \pmod{11} \end{aligned} \tag{2.1}$$

Logo, pela proposição 2.2, o logaritmo possui solução. Resolvendo o logaritmo, temos:

$$x = \log_7 9 \Leftrightarrow 7^x \equiv 9 \pmod{11}$$

Como se pode ver em (2.1), $9 \equiv 7^8 \pmod{11}$, portanto, $x = 8$.

□

Vejamos um exemplo mais elaborado.

Exemplo 2.2. *O número* $p = 87557$ *é primo e podemos verificar que 3 é gerador de* $\mathbb{Z}_{87557}^*$. *Calcule o logaritmo discreto de 27634.*

Solução:

Desejamos calcular $x = \log_3 27634$ em $\mathbb{Z}_{87557}$. O método óbvio seria calcular todas as potências

$$3^1, 3^2, 3^3, ..., 3^{87556} \pmod{87557}$$

para encontrarmos algum potência de 3 congruente a 27634. Fazer este calculo manualmente é inviável, pois demanda muito tempo, mas utilizando um computador[2] encontramos que

$$3^{24890} \equiv 27634 \ (\mathrm{mod}\ 87557)$$

Logo, temos em $\mathbb{Z}_{87557}$, $\log_3 27634 = 24890$.

□

Neste exemplo foram utilizados valores baixos, o que torna o problema de fácil resolução via computador. Entretanto, quando o primo p e o gerador a de $\mathbb{Z}_p^*$ são convenientemente escolhidos (sobretudo com p possuindo uma grande quantidade de algarismos), a resolução torna-se difícil até mesmo para um computador. Esta dificuldade inspirou Diffie e Hellman a criarem um protocolo de encriptação baseado no problema do logaritmo discreto, que veremos na próxima seção.

2.1 Protocolo Diffie-Hellman

O protocolo Diffie-Hellman, publicado em 1976 por W. Diffie e M. E. Hellman [4], propõe um modelo que combina criptografia simétrica ao problema do logaritmo discreto para realizar a troca de chaves. O protocolo consiste em realizar a troca de chave para criptografia simétrica por um canal inseguro de tal forma que, mesmo que um intruso intercepte a chave compartilhada, seja inviável determinar as chaves secretas e, consequentemente, decifrar a mensagem.

Textos sobre o tema critografia usualmente denominam o emissor de Alice, o receptor de Bob e o intruso de Carlos para facilitar a compreensão. Neste trabalho, também seguiremos esta nomenclatura. Vejamos os passos para a criação e compartilhamento da chave.

1. Inicialmente, Alice e Bob 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. Alice escolhe um inteiro a, $1 \leq a \leq p-2$, que não será divulgado.

[2] ver Apêndice A

3. Bob escolhe um inteiro b, $1 \leq b \leq p-2$, que também não será divulgado.

4. Alice escolhe um inteiro $A \equiv g^a \pmod{p}$ e o envia para Bob.

5. Bob escolhe um inteiro $B \equiv g^b \pmod{p}$ e o envia para Alice.

6. Alice, então, escolhe uma chave $K_A \equiv B^a \pmod{p}$.

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

7. Bob, por sua vez, escolhe uma chave $K_B \equiv A^b \pmod{p}$.

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

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

Como se pode ver, Alice e Bob possuem a mesma chave para codificação e decodificação, mas em nenhum momento esta chave K_{AB} foi transmitida de fato. Após executar este protocolo, a comunicação pode ser realizada utilizando um criptossistema de chave secreta qualquer.

Empregando a notação da definição 1.3.2, para codificar uma mensagem $M \in \mathcal{P}$, deve-se aplicar a função de codificação

$$E_{K_{AB}} : \mathcal{P} \to \mathcal{C}$$

$$x \mapsto K_{AB}.x \pmod{p}$$

à mensagem M, gerando a mensagem cifrada M':

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

Para decodificar a mensagem $M' \in \mathcal{C}$, deve-se aplicar a função de decodificação a M', ou seja, $D_{K_{AB}}(M')$, que utiliza o inverso de K_{AB} módulo p, ${K_{AB}}^{-1}$.

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

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

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

$$D_{K_{AB}}(M') \equiv M \ (\mathrm{mod}\ p)$$

Suponhamos que Carlos consiga interceptar a chave que Alice envia a Bob, neste caso a única informação sobre a chave de que ele tem conhecimento é

$$A \equiv g^a \ (\mathrm{mod}\ p)$$

Carlos conhece os inteiros p e g, mas não conhece a. Para determinar este valor, precisa calcular o logaritmo discreto $a = \log_g A \ (\mathrm{mod}\ p)$, o que é inviável.

De modo análogo, se Carlos receptasse a transmissão de Bob a Alice, teria a seguinte informação:

$$B \equiv g^b \ (\mathrm{mod}\ p)$$

o que implica em calcular o logaritmo discreto $b = \log_g B \ (\mathrm{mod}\ p)$, o que também é inviável, pois Carlos não conhece o inteiro b e p é um primo com grande quantidade de algarismos. Deste modo, o problema do logaritmo discreto contribui para a segurança na troca de chaves pelo protocolo Diffie-Hellman.

2.2 Criptossistema de Chave Pública ElGamal

Um cripstossistema de chave pública baseado no Problema do Logaritmo Discreto foi proposto por Taher ElGamal em 1985 no artigo *A public key cryptosystem and a signature scheme based on discrete logarithms.* Ao contrário do protocolo Diffie-Hellman, tratado na seção anterior, o ElGamal utiliza chave assimétrica. Empregando a notação da definição 1.3.2, temos:

Definição 2.2.1 (Criptossistema ElGamal)**.** *Sejam p um primo, $g \in \mathbb{Z}_p$ um gerador de $\mathbb{Z}_p^*$ e $a \in \mathbb{Z}_p$. Seja $\mathcal{P} = \mathbb{Z}_p$ e $\mathcal{C} = \mathbb{Z}_p \times \mathbb{Z}_p$ e*

$$\mathcal{K} = (p, g, a, A) : A \equiv g^a \ (\mathrm{mod}\ p)$$

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

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

com

$$y_1 \equiv g^k \ (\mathrm{mod}\ p)$$

$$y_2 \equiv xA^k \ (\mathrm{mod}\ p)$$

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

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

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

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

Em termos práticos, suponhamos que Bob deseja enviar uma mensagem M a Alice. Para isto, Alice e Bob combinam de utilizar um primo p convenientemente longo e um inteiro g, gerador de $\mathbb{Z}_p^*$, sendo que estes valores são públicos. A comunicação ocorre como segue:

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

$$A \equiv g^a \ (\mathrm{mod}\ p)$$

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

$$y_1 \equiv g^k \ (\mathrm{mod}\ p) \quad \text{e} \quad y_2 \equiv M.A^k \ (\mathrm{mod}\ p)$$

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

Note que no passo 1, o valor a escolhido por Alice precisa ser diferente de $p-1$ pois, pelo teorema 1.5, $g^{\phi(p)} \equiv 1 \ (\mathrm{mod}\ p)$ e como $\phi(p) = p-1$, teríamos $A \equiv g^{p-1} \equiv 1 \ (\mathrm{mod}\ p)$, logo, y_2 seria a própria mensagem M e não faria sentido cifrar esta mensagem. Pelo mesmo motivo, deve-se ter $k < p-1$. O valor A também é considerado público, pois pode ser interceptado facilmente. Apesar disto, a segurança não é comprometida, pois Carlos, um intruso, terá dificuldade para decifrar a mensagem original.

Caso Carlos consiga o valor A, considerando que p e g são conhecidos, precisaria resolver $\log_g A \ (\mathrm{mod}\ p)$ para determinar a chave secreta a, o que já sabemos ser inviável. Além

disso, se Carlos interceptar a mensagem (y_1, y_2), deverá determinar $k = \log_g y_1 \pmod p$, ou seja, determinar dois logaritmos discretos igualmente inviáveis de resolver.

Para decodificar a mensagem (y_1, y_2) recebida, Alice precisa executar os seguintes passos:

1. Determina $x \equiv (y_1)^a \pmod p$ e seu inverso x^{-1} módulo p.
2. Calcula $y_2 x^{-1}$ para encontrar a mensagem original

$$y_2 x^{-1} \equiv (M.A^k)x^{-1} \equiv M(g^a)^k x^{-1} \equiv M(g^k)^a x^{-1}$$

$$\equiv M(y_1)^a x^{-1} \equiv M.x.x^{-1} \equiv M \ (\mathrm{mod}\ p)$$

Deste modo, após estas operações Alice consegue ler a mensagem original.

Quando a mensagem codificada é um texto, usualmente utiliza-se a tabela ASCII para converter a mensagem em um valor numérico, afim de efetuar as operações necessárias para codificação e decodificação.

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

Vejamos um exemplo numérico:

Exemplo 2.3. *Codificar a palavra PAI, utilizando* $p = 817.123$ *e* $g = 13$.

Solução:

Vamos, incialmente, converter a palavra PAI utilizando a tabela ASCII da figura 2.1. Para efeitos de simplificação, consideraremos apenas dois dígitos para cada letra:

- P = 80
- A = 65
- I = 73

Logo, a palavra PAI corresponde a 806.573. Seja $a = 5$, temos:

$$A \equiv 13^5 \equiv 371.293 \ (\text{mod } 817.123)$$

Neste caso, temos a chave $K = (817.123, 13, 5, 371.293)$. Façamos $k = 2$, temos:

$$y_1 \equiv 13^2 \equiv 169 \ (\text{mod } 817.123)$$

$$y_2 \equiv 806.573(371.293)^2 \equiv 550.537 \ (\text{mod } 817.123)$$

Logo, a mensagem cifrada é $(169, 550.537)$.

□

Para decifrar esta mensagem, seguimos os passos:

1. $x \equiv 169^5 \equiv 36.273 \ (\text{mod } 817.123)$
2. $x^{-1} \equiv x^{817.123-2} \equiv 36.273^{817.121} \equiv 371.268 \ (\text{mod } 817.123)$
3. $y_2 x^{-1} = 550.537 \times 371.268 = 204.396.770.916 \equiv 806.573 \ (\text{mod } 817.123)$

Separando este último resultado em blocos de dois dígitos e convertendo de acordo com a tabela da figura 2.1, encontramos a mensagem original:

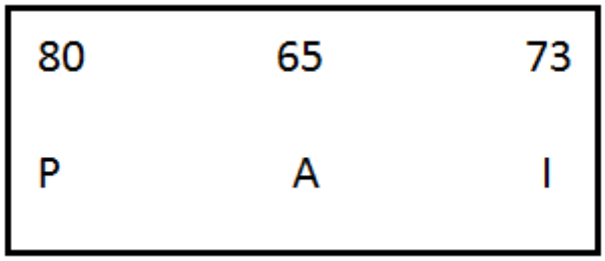

Figura 2.2: Mensagem decodificada

Agora que já temos o Problema do Logaritmo Discreto bem definido e sabemos como aplicá-lo, passaremos a abordar as curvas elípticas.

Capítulo 3

CURVAS ELÍPTICAS

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \tag{3.1}$$

com $a_1, a_2, a_3, a_4, a_5 \in \mathbb{K}$.

Porém, para o escopo deste trabalho, trabalharemos com curvas elípticas simétricas em relação ao eixo-x e sem singularidades, pois precisaremos que as mesmas tenham retas tangentes em todos os seus pontos. Deste modo, trabalharemos com uma versão simplificada da equação (3.1).

3.1 Equação de Weierstrass Simplificada

Definição 3.1.1. *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 $4A^3 + 27B^2 \neq 0$.

A condição $4A^3 + 27B^2 \neq 0$ é necessária para que a curva não tenha singularidades. De fato, derivando a equação $y^2 = x^3 + Ax + B$ em relação a x, temos:

$$2y\frac{dy}{dx} = 3x^2 + A$$

$$\frac{dy}{dx} = \frac{3x^2 + A}{2y} \tag{3.2}$$

Para que a derivada $\frac{dy}{dx}$ exista, devemos ter $y \neq 0$. Vejamos o que ocorre nos pontos críticos da curva, ou seja, nos nos pontos em que a derivada $\frac{dy}{dx}$ é zero. Temos, então, $3x^2 + A = 0$ na equação (3.2), logo:

$$x = \pm\sqrt{-\frac{A}{3}} \tag{3.3}$$

Fazendo $y = 0$, temos que a derivada da equação (3.2) não existe e, portanto, a curva não é diferenciável. Se tivéssemos $y = 0$, teríamos que $y^2 = 0$. Logo, da definição 3.1.1:

$$x^3 + Ax + B = 0$$

$$x(x^2 + A) + B = 0$$

Substituindo (3.3) na equação acima, temos:

$$\left(\pm\sqrt{-\frac{A}{3}} \right) \left(-\frac{A}{3} + A \right) + B = 0$$

$$\left(\pm\sqrt{-\frac{A}{3}} \right) \left(\frac{2A}{3} \right) = -B$$

$$\left(-\frac{A}{3} \right) \left(\frac{4A^2}{9} \right) = B^2$$

$$\frac{-4A^3}{27} = B^2$$

$$-4A^3 = 27B^2$$

$$4A^3 + 27B^2 = 0$$

Portanto, para que a curva exista, devemos ter $4A^3 + 27B^2 \neq 0$. Esta condição é necessária e suficiente para que a curva não tenha singularidades. A condição acima garante, ainda, que a equação não possui raízes múltiplas.

Se consideramos curvas elípticas sobre $\mathbb{R}$, podemos traçar o gráfico no plano cartesiano. Vejamos alguns exemplos de curvas elípticas.

Exemplo 3.1. *Seja a curva elíptica $E(\mathbb{R})$ de equação $y^2 = x^3 - 2x + 2$. Verifique se a curva satisfaz a condição da definição 3.1.1.*

Solução:

Vejamos se a equação $y^2 = x^3 - 2x + 2$ satisfaz a condição $4A^3 + 27B^2 \neq 0$. Neste caso, temos $A = -2$ e $B = 2$.

$$4.(-2)^3 + 27.2^2 = 4.(-8) + 27.4 = -32 + 108 = 76 \neq 0$$

Logo, a curva $E(\mathbb{R})$ satisfaz a condição da definição 3.1.1.

□

O gráfico desta curva pode ser visto na figura 3.1

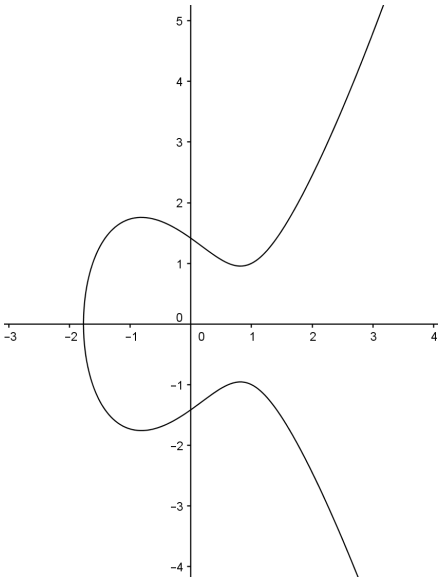

Figura 3.1: Gráfico da curva $y^2 = x^3 - 2x + 2$

Conforme se pode observar na figura 3.1, a curva possui apenas uma raiz real. Vejamos um exemplo de curva com três raízes reais distintas.

Exemplo 3.2. *Mostre que a curva $E(\mathbb{R})$ de equação $y^2 = x^3 - 4x + 3$ não possui singularidades.*

Solução:

Para que uma curva não possua singularidades é suficiente que tenhamos $4A^3+27B^2 \neq 0$. No caso da curva em questão, temos $A = -4$ e $B = 3$, logo:

$$4.(-4)^3 + 27.3^2 = 4.(-64) + 27.9 = -256 + 243 = -13 \neq 0$$

Portanto, a curva não possui singularidades.

□

O gráfico desta curva pode ser visto na figura 3.2 a seguir.

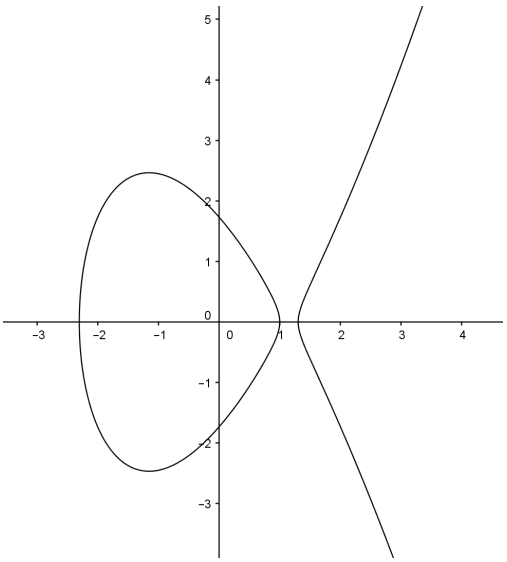

Figura 3.2: Gráfico da curva $y^2 = x^3 - 4x + 3$

Como se pode ver, o gráfico da curva intersecta o eixo-x em três pontos diferentes, o que significa que a equação da curva possui três raízes reais distintas. No exemplo 3.3, mostramos um exemplo de curva com raízes duplas.

Exemplo 3.3. *Verifique se a curva sobre* $\mathbb{R}$ *de equação* $y^2 = x^3 - 3x + 2$ *satisfaz a condição da definição 3.1.1.*

Solução

Vejamos se a condição $4A^3 + 27B^2 \neq 0$ é verdadeira para a curva com $A = -3$ e $B = 2$:

$$4.(-3)^3 + 27.2^2 = 4.(-27) + 27.4 = -108 + 108 = 0$$

Portanto, esta curva não se encaixa na definição 3.1.1[1].

[1]Equações deste tipo são chamadas de equações cúbicas singulares. Ver SILVERMAN[11], página 43

□

Isto significa que a equação cúbica $y^2 = x^3 - 3x + 2$ possui uma raiz real dupla. Observe o gráfico na figura 3.3.

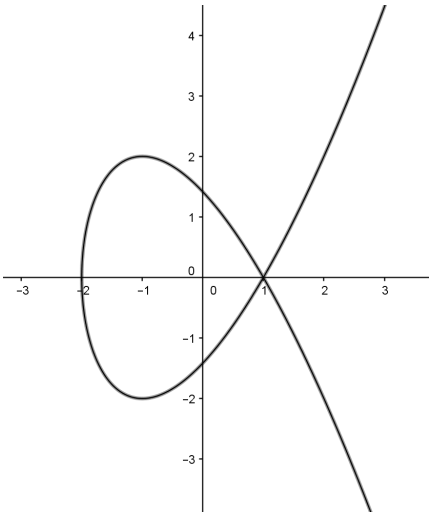

Figura 3.3: Gráfico da curva $y^2 = x^3 - 3x + 2$

As raízes da equação, como se pode concluir da figura 3.3, são -2 e 1, sendo que 1 é uma raiz dupla. Como veremos na seção 3.2, curvas deste tipo não servem para o propósito deste trabalho, pois não possuem reta tangente nos pontos de singularidade.

Podemos definir uma operação de soma entre dois pontos de uma curva $E(\mathbb{K})$ e, desta forma, transformá-la em um grupo abeliano.

3.2 Soma de pontos em curvas elípticas

A soma de dois pontos em uma curva elíptica pode ser tratada tanto de forma geométrica quanto algébrica. Vejamos, inicialmente, a forma geométrica. Para tornar o texto mais didático, analisaremos curvas $E(\mathbb{R})$ sobre o corpo dos reais, mas as propriedades a seguir são válidas para curvas sobre qualquer corpo $\mathbb{K}$

Sejam dois pontos $P, Q \in E(\mathbb{R})$. Considere a reta r que passa pelos pontos P e Q, tal que r não seja uma reta vertical[2]. Temos que a reta r intersecta a curva $E(\mathbb{R})$ em um

[2]O caso que a reta r é vertical, ou seja, paralela ao eixo-y será analisado quando definirmos o elemento neutro da operação de soma entre dois pontos

terceiro ponto R'.

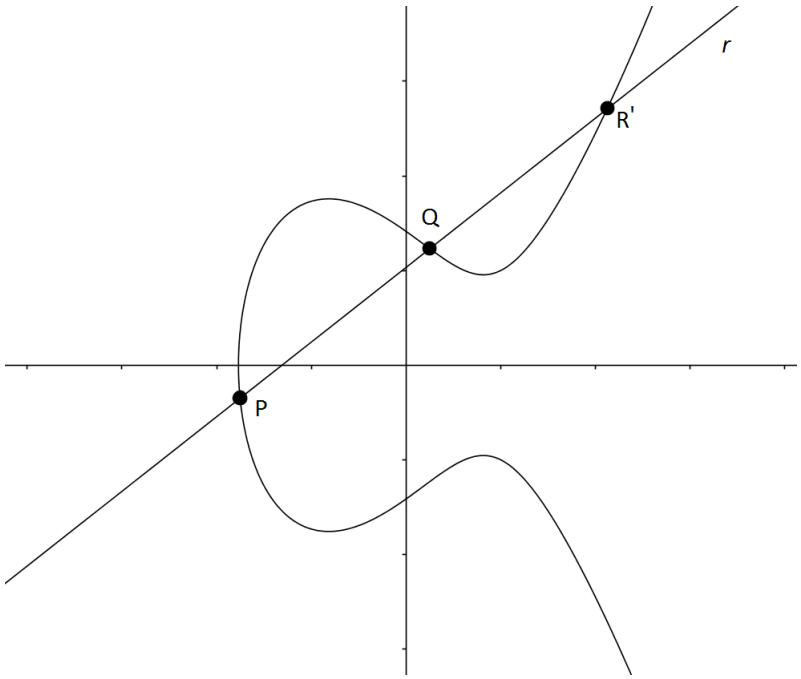

Figura 3.4: Soma de dois pontos em uma curva $E(\mathbb{R})$

Como a curva é simétrica em relação ao eixo horizontal, temos que a reflexão do ponto R' em relação ao eixo horizontal pertence à curva. Chamemos este ponto de R, dizemos que $R = P + Q$.

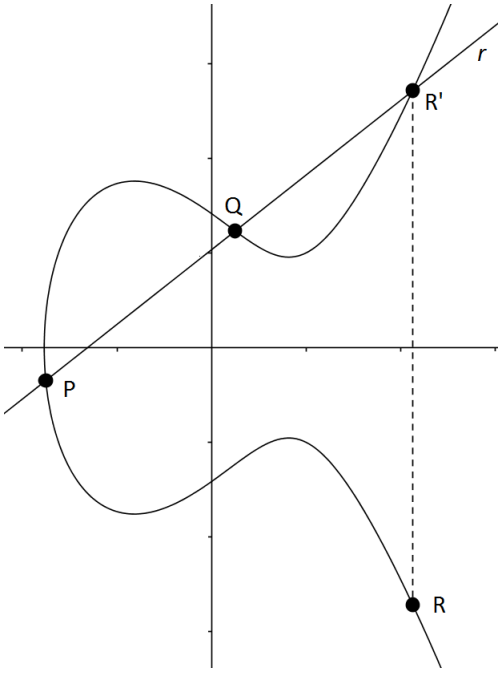

Figura 3.5: Soma de dois pontos em uma curva $E(\mathbb{R})$: $R = P + Q$

Para que a curva $E(\mathbb{R})$ com a operação de soma de dois pontos em curva seja um grupo abeliano, de acordo com a seção 1.2, devemos ter um elemento neutro para esta operação. Para isto, definimos um ponto O, chamado *Ponto no Infinito*[3], não pertecente ao plano $\mathbb{R}^2$, tal que O esteja em toda reta vertical do $\mathbb{R}^2$, ou seja, O pertence a todas as retas $x = k$, com $k \in \mathbb{R}$.

Para que seja possível realizar uma soma $P+O$, consideramos que o ponto O também pertence à curva $E(\mathbb{R})$. Deste modo,ao fazermos $P + O$, teremos que a reta que passa por estes pontos é vertical e intersecta a curva $E(\mathbb{R})$ no ponto P', que é a reflexão do ponto P em relação ao eixo horizontal, devido à simetria da curva.

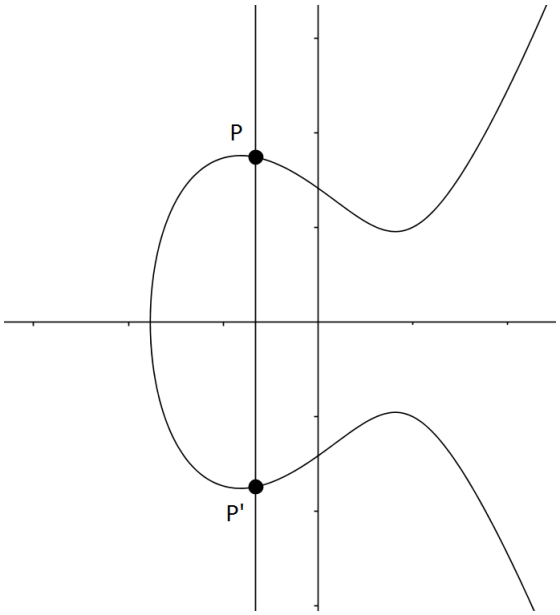

Figura 3.6: Soma entre um ponto P e o ponto no infinito O: $P + O$

Como se pode ver na figura 3.6, a reflexão do ponto P' em relação ao eixo horizontal é o próprio ponto P, logo, temos que

$$P + O = P$$

portanto, o ponto O é o elemento neutro da operação de soma entre dois pontos de uma curva elíptica.

[3]Também chamado de ponto impróprio.

Observe que o ponto P' é o inverso aditivo de P, pois a reta que passa por P e P' é vertical e, portanto, o terceiro ponto de interseção com a curva é o ponto O, ou seja:

$$P + P' = O$$

Neste trabalho, o ponto P', inverso aditivo de P, será representado por $-P$.

Também podemos determinar uma soma $P + P$, para isto tomamos a reta tangente à curva no ponto P. Neste caso, a reta tangente em P intersecta a curva em um segundo ponto R' e temos que a reflexão R em relação ao eixo horizontal é o ponto desejado, ou seja, $R = P + P$. Também podemos representar a soma $P + P$ como $2P$.

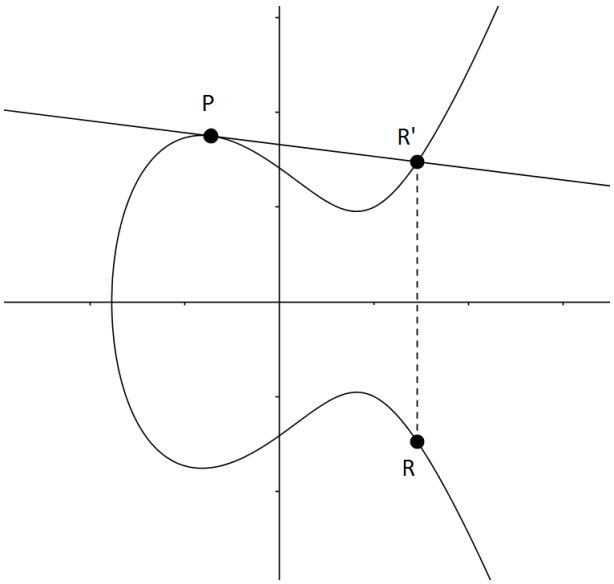

Figura 3.7: $R = P + P$ ou $R = 2P$

Um caso especial ocorre quando a reta tangente no ponto P é vertical. Como o ponto $O \in E(\mathbb{R})$ pertence a todas as retas verticais do plano, temos que O também pertence à reta tangente em P. Logo:

$$P + P = O$$

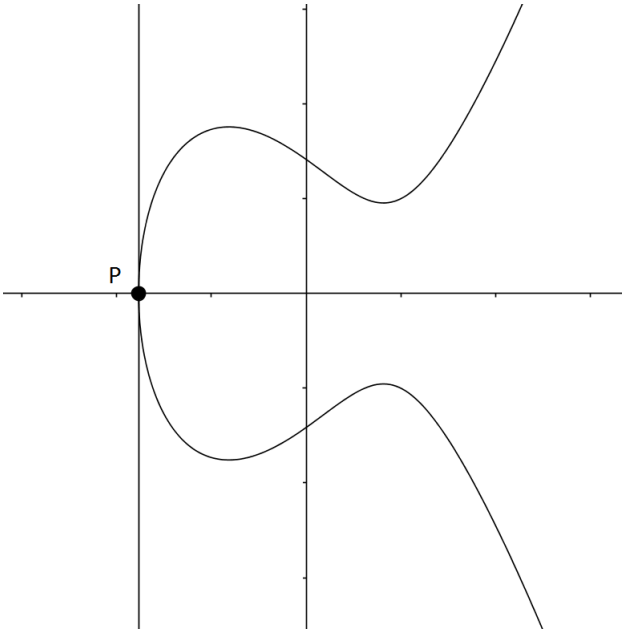

Figura 3.8: $P + P$ quando a reta tangente é vertical.

3.2.1 Soma algébrica

Podemos, também, trabalhar com as coordenadas dos pontos em uma curva elíptica. Sejam $P = (x_p, y_p)$ e $Q = (x_q, y_q)$ dois pontos de uma curva elíptica $E(\mathbb{R})$ de equação $y^2 = x^3 + Ax + B$, com $4A^3 + 27B^2 \neq 0$, com $P \neq O$ e $Q \neq O$. Tomemos $P \neq Q$ (trataremos o caso $P = Q$ posteriormente). Seja r a reta que passa pelos pontos P e Q, sabemos que esta reta intersecta a curva $E(\mathbb{R})$ em um terceiro ponto $R' = (x'_r, y'_r)$.

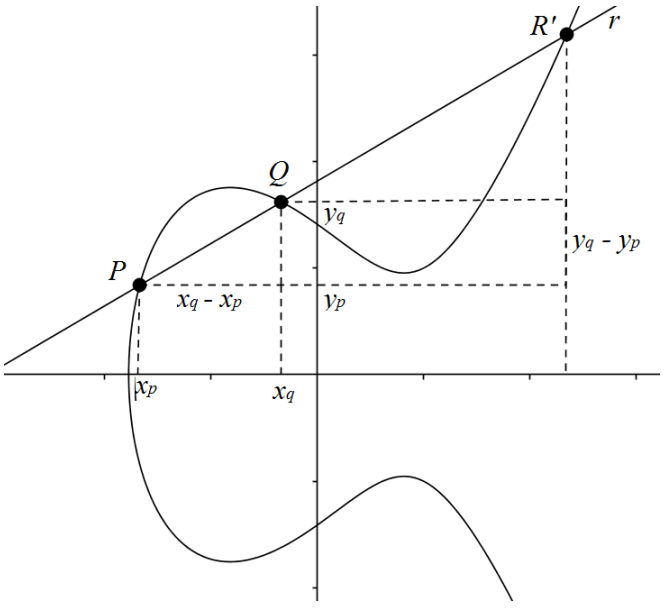

Figura 3.9: Reta que passa pelos pontos P e Q.

Da figura 3.9 conclui-se que a inclinação da reta r é

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

com $x_q \neq x_p$ (se $x_q = x_p$, temos uma reta vertical, ver figura 3.6).

Deste modo, a equação da reta r é

$$y = m(x - x_p) + y_p \tag{3.4}$$

pois r passa pelo ponto P. Para determinarmos as interseções entre a reta r e a curva $E(\mathbb{R})$, basta substituirmos a equação da reta na equação da curva. Temos:

$$(m(x - x_p) + y_p)^2 = x^3 + Ax + B$$

$$m^2x^2 - 2m^2x_px + m^2x_p^2 + my_px - mx_py_p + y_p^2 = x^3 + Ax + B$$

$$x^3 - m^2x^2 + (A + 2m^2x_p - my_p)x + (B - m^2x_p^2 + mx_py_p - y_p^2) = 0$$

Fazendo $a = -m^2$, $b = A + 2m^2x_p - my_p$ e $c = B - m^2x_p^2 + mx_py_p - y_p^2$ temos a seguinte equação cúbica:

$$x^3 + ax^2 + bx + c = 0 \tag{3.5}$$

Como os pontos P, Q e R' são as interseções da reta r com a curva $E(\mathbb{R})$, temos que x_p, x_q e x'_r são as raízes da equação (3.5). Aplicando as Relações de Girard, temos que a soma das raízes é

$$-a = x_p + x_q + x'_r$$

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

$$m^2 = x_p + x_q + x'_r$$

$$x'_r = m^2 - x_p - x_q \tag{3.6}$$

Como $R' \in r$, podemos substituir suas coordenadas na equação (3.4). Portanto:

$$y'_r = m(x'_r - x_p) + y_p \tag{3.7}$$

Conforme definimos na seção 3.2, o ponto $R = P + Q$, $R = (x_r, y_r)$, é a reflexão de R' em relação ao eixo horizontal, ou seja, $x_r = x'_r$ e $y_r = -y'_r$. Substituindo, respectivamente, em (3.6) e (3.7), temos:

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

e

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

Consideremos, agora, o caso em que temos $P = Q$, temos que a reta r é tangente à curva no ponto P. Deste modo, a inclinação da reta será a derivada no ponto P em relação a x. Conforme se pode concluir da equação (3.2), temos para (x_p, y_p):

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

com $y_p \neq 0$, caso contrário, assume-se que a reta é vertical e, conforme vimos na seção 3.2, teremos $P + P = O$.

Sendo assim, a reta r que passa por P com inclinação m tem a mesma forma da equação (3.4): $y = m(x - x_p) + y_p$. Deste modo, ao fazermos a interseção desta reta com a curva $E(\mathbb{R})$ obteremos novamente a equação (3.5), com a diferença de que agora as raízes não são todas distintas, pois x_p é uma raiz dupla. Deste modo, temos, aplicando as Relações de Girard, que

$$m^2 = x_p + x_p + x'_r$$

$$x_r = x'_r = m^2 - 2x_p$$

Para determinar y_r, o raciocínio é o mesmo empregado no caso $P \neq Q$ e temos

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

No caso em que temos $P = O$, teremos $x_r = x_p$ e $y_r = y_p$ e no caso $Q = O$, teremos $x_r = x_q$ e $y_r = y_q$, já que o ponto O serve como elemento neutro para a operação.

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

Definição 3.2.1 (Soma de dois pontos de uma curva elíptica em termos algébricos)**.** *Seja $E(\mathbb{R})$ 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 $E(\mathbb{R})$ tais que $R = P + Q$.*

1. *Se $P = O$, então $R = Q$*
2. *Se $Q = O$, então $R = P$*
3. *Se $x_p = x_q$ e $y_p = -y_q$, então $R = O$*

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

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

Vejamos um exemplo de aplicação da soma algébrica.

Exemplo 3.4. *Considere a curva $E(\mathbb{R})$ de equação $y^2 = x^3 - 3x + 1$ e os pontos $P = (0, 1)$ e $Q = (2, \sqrt{3})$. Determine as coordenadas do ponto $R \in E(\mathbb{R})$ tal que $R = P + Q$.*

Solução:

A figura a seguir mostra o gráfico de $E(\mathbb{R})$ e a soma geométrica $P + Q$

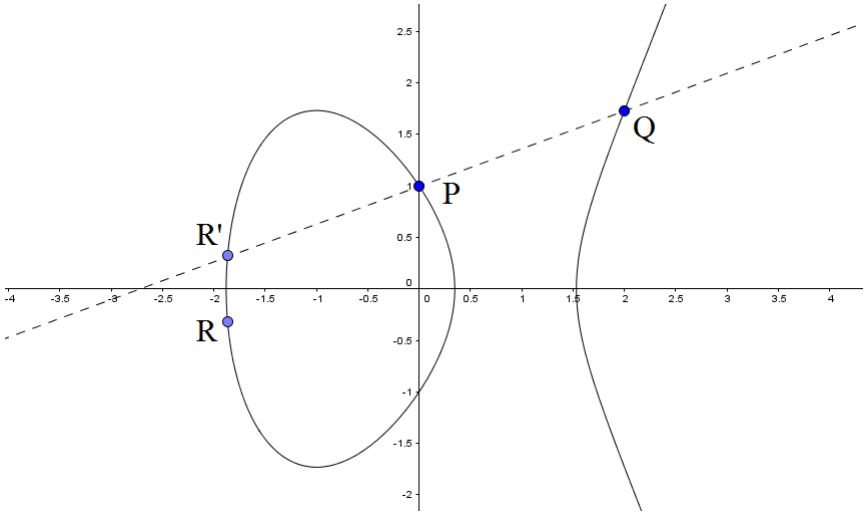

Figura 3.10: Gráfico de $y^2 = x^3 - 3x + 1$.

Aplicando a definição 3.2.1, temos:

$$m = \frac{y_q - y_p}{x_q - x_p}, \quad \text{pois } P \neq Q$$

$$m = \frac{\sqrt{3} - 1}{2 - 0}$$

$$m = \frac{\sqrt{3} - 1}{2}$$

Deste modo:

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

$$x_r = \left(\frac{\sqrt{3} - 1}{2} \right)^2 - 0 - 2$$

$$x_r = \frac{4 - 2\sqrt{3}}{4} - 2$$

$$x_r = -\frac{\sqrt{3}}{2} - 1$$

Calculando y_r, temos:

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

$$y_r = \left(\frac{\sqrt{3} - 1}{2} \right) \left(0 + \frac{\sqrt{3}}{2} + 1 \right) - 1$$

$$y_r = \frac{1}{4}(1 + \sqrt{3}) - 1$$

$$y_r = \frac{\sqrt{3}-3}{4}$$

Portanto, temos $R = \left(-\frac{\sqrt{3}}{2} - 1, \frac{\sqrt{3}-3}{4} \right)$.

□

Como a operação de soma está bem definida, podemos verificar o seguinte:

Proposição 3.1. *$(E(\mathbb{K}), +)$, onde $+$ é a operação de soma entre dois pontos de $E(\mathbb{K})$, é um grupo abeliano.*

Demonstração:

De acordo com a seção 1.2, um grupo abeliano precisa satisfazer as seguintes propriedades:

P1. associativa;

P2. possuir elemento neutro;

P3. possuir elemento inverso;

P4. comutativa.

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

P1: Associatividade

A prova da associatividade é extensa, pois, dados três pontos P, Q e $R \in E(\mathbb{K})$, para mostrarmos que $(P + Q) + R = P + (Q + R)$, devemos considerar os casos em que $P = Q$, $P = R$, $Q = R$, $P + Q = R$, $P = Q + R$ e $P \neq Q \neq R$, o que foge do escopo deste trabalho. Uma demonstração completa pode ser encontrada em WASHINGTON [16], página 20.

P2: Existência do Elemento Neutro

Como vimos na seção 3.2, o ponto O é o elemento neutro da soma entre dois pontos de uma curva elíptica e para qualquer $P \in E(\mathbb{K})$, temos $P + O = O + P = P$, logo, existe

elemento neutro.

P3: Existência do Elemento Inverso

Seja um ponto P qualquer da curva e um ponto $-P$ tal que $-P$ é a reflexão de P em relação ao eixo horizontal. A reta que passa por P e $-P$ é vertical e, conforme vimos na seção 3.2, $P + (-P) = (-P) + P = O$, portanto, existe o inverso aditivo.

P4: Comutatividade

A comutatividade é óbvia, visto 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.

□

Como a operação de soma é válida para qualquer corpo $\mathbb{K}$, podemos trabalhar com curvas sobre corpos finitos. Para o escopo deste trabalho, trabalharemos com curvas sobre o corpo $\mathbb{Z}_p$.

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

Uma curva elíptica sobre o corpo $\mathbb{Z}_p$, segundo a definição 3.1.1, 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 $4A^3 + 27B^2 \not\equiv 0 (\text{mod } p)$, incluindo o ponto no infinito O.

Uma curva $E(\mathbb{Z}_p)$ claramente 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 (devido à simetria da curva). Sendo assim, acrescentando o ponto O, uma curva sobre $\mathbb{Z}_p$ possui, no máximo, 2p+1 pontos[4].

[4] O Teorema de Hasse-Weil melhora esta estimativa, dizendo que o total de pontos de uma curva elíptica sobre $\mathbb{Z}_p$ é menor do que ou igual a $p + 1 + 2\sqrt{p}$ ver[11, 16]

Como uma curva $E(\mathbb{K})$ é um conjunto finito de pontos, podemos determinar todos eles.

Exemplo 3.5. *Determine todos os pontos da curva $E(\mathbb{Z}_{11})$ de equação $y^2 = x^3 - x + 3$.*

Solução:

Para determinar se um ponto pertence à curva, tomamos cada valor possível de x, substituímos em $x^3 - x + 3 \mod (11)$ e verificamos se este resultado é o quadrado módulo 11 de algum y. A tabela abaixo com todos os valores possíveis de x e y facilita a visualização.

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 ver, por exemplo, que para $x = 7$, temos $x^3 - x + 3 \equiv 9 \mod (11)$, que por sua vez é quadrado módulo 11 de $y = 3$ e $y = 8$. Portanto, os pontos $(7, 3)$ e $(7, 8)$ pertencem a curva. Observe 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 $2 \mod (11)$, ou seja, nenhum ponto da curva tem coordenada $x = 5$. Analisando todos os valores possíveis, encontramos os seguintes pontos:

$$(0,5) \quad (0,6) \quad (1,5) \quad (1,6) \quad (2,3) \quad (2,8) \quad (3,3) \quad (3,7)$$

$$(6,2) \quad (6,9) \quad (7,3) \quad (7,8) \quad (8,1) \quad (8,10) \quad (10,5) \quad (10,6)$$

□

Obviamente, quanto maior o primo p escolhido, mais inviável se torna determinar todos os pontos de $E(\mathbb{Z}_p)$. Ao trabalharmos com curvas sobre $\mathbb{Z}_p$, não faz sentido falarmos em gráfico da curva, pois a mesma se torna uma plotagem de pontos. Na figura 3.11 podemos ver a plotagem da curva $E(\mathbb{Z}_{23})$ de equação $y^2 = x^3 + 9x + 17$.

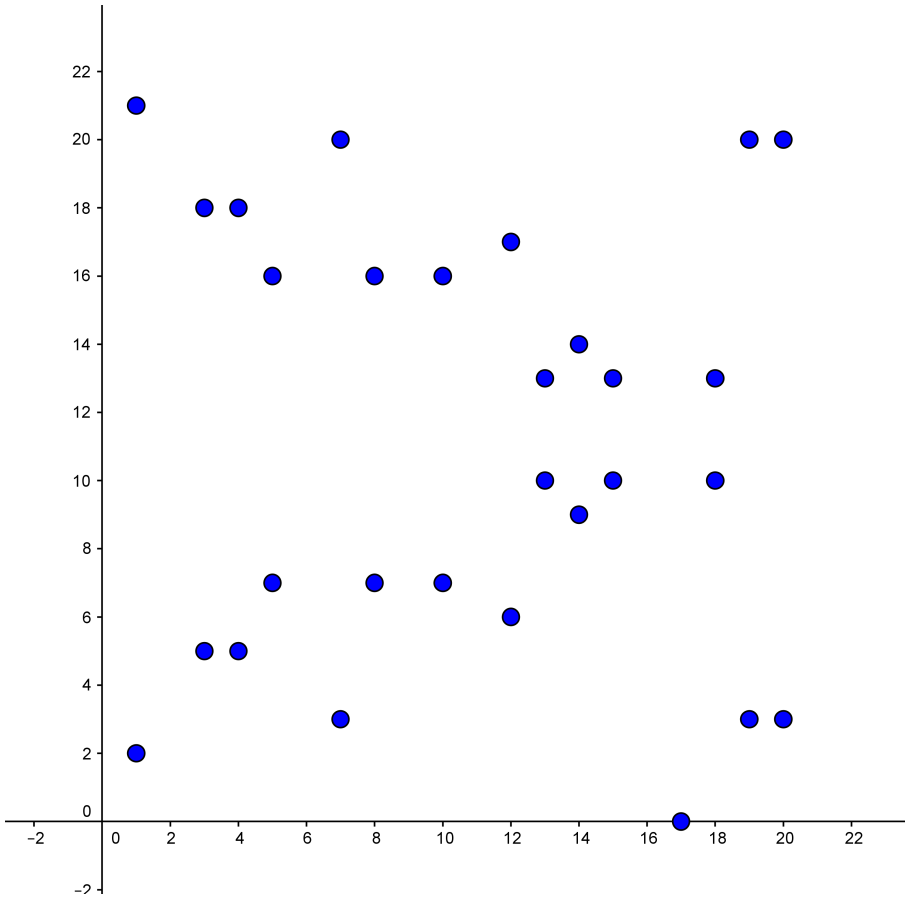

Figura 3.11: Plotagem de uma curva sobre $\mathbb{Z}_{23}$.

Quando lidamos com curvas sobre $\mathbb{Z}_p$, empregamos a soma entre dois pontos na forma algébrica. Vejamos um exemplo:

Exemplo 3.6. *Seja a curva $E(\mathbb{Z}_{11})$ de equação $y^2 = x^3 - x + 3$ e os pontos $P = (1, 5)$ e $Q = (8, 10)$ pertencentes a curva. Calcule as coordenadas do ponto $R = P + Q$.*

Solução

Para somar os pontos basta aplicar a definição 3.2.1. Como $P \neq Q$ e $x_p \neq x_q$:

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

$$m = \frac{10-5}{8-1}$$
$$m = \frac{5}{7}$$

Estamos trabalhando em $\mathbb{Z}_{11}$, isto significa que m é o inteiro tal que $7m \equiv 5 \mod (11)$, logo, $m = 7$, pois $7.7 = 49 \equiv 5 \mod (11)$.

Calculando a coordenada x_r:

$$x_r = m^2 - x_p - x_q$$
$$x_r = 7^2 - 1 - 8$$
$$x_r = 40 \equiv 7 \mod (11)$$

Para y_r:

$$y_r = m(x_p - x_r) - y_p$$
$$y_r = 7(1-7) - 5$$
$$y_r = -47 \equiv 8 \mod (11)$$

Logo, temos $R = (7, 8)$. Como podemos ver no exemplo 3.5, $R \in \mathbb{Z}_{11}$.

□

3.4 O problema do logaritmo discreto elíptico

Conforme vimos na seção 3.2, ao somarmos $P+P$ encontramos um ponto $2P$, múltiplo de P. Se tomarmos este resultado e somarmos P novamente, ou seja, $2P + P$, teremos como resultado um ponto que denominaremos $3P$. Fazendo este procedimento n vezes, com $n \in \mathbb{N}$, temos:

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

Deste modo, dado um ponto $P \in E(\mathbb{Z}_p)$, podemos determinar os múltiplos $2P$, $3P$, $4P$, $\ldots$, nP deste ponto P. Vejamos um exemplo.

Exemplo 3.7. *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

Empregando o mesmo procedimento utilizando no exemplo 3.5, encontramos que os pontos da curva em questão são:

$$(0,5) \quad (0,8) \quad (5,2) \quad (5,11)$$

$$(11,0) \quad (12,3) \quad (12,10)$$

Portanto, $P \in E(\mathbb{Z}_{13})$.

Para determinar os múltiplos de P, empregamos a definição algébrica de soma. Vejamos:

$$2P = P + P = (5,2) + (5,2) = (12,3)$$
$$3P = 2P + P = (12,3) + (5,2) = (0,8)$$
$$4P = 3P + P = (0,8) + (5,2) = (11,0)$$
$$5P = 4P + P = (11,0) + (5,2) = (0,5)$$
$$6P = 5P + P = (0,5) + (5,2) = (12,10)$$
$$7P = 6P + P = (12,10) + (5,2) = (5,11)$$
$$8P = 7P + P = (5,11) + (5,2) = O^5$$

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

□

No exemplo 3.7, 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 (cíclico), dizemos que P é um *gerador* do grupo. É importante notar que nem todo ponto de uma curva possui múltiplos, além disso, algum ponto pode não ser múltiplo de outro. Por exemplo, o ponto $(11,0)$ na curva do exemplo anterior não possui múltiplos[6].

[5] $11 \equiv -2 \mod 13$, logo esta soma cai no caso 3 da definição 3.2.1

[6] De forma geral, pontos da curva $E(\mathbb{Z}_p)$ que possuem a forma $(k,0)$, com $k \in \mathbb{Z}$, não possuem múltiplos, pois a reta tangente neste ponto é sempre vertical. Ver figura 3.8

Podemos adaptar 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 $E(\mathbb{Z}_p)$. Deste modo, para cada $Q \in E(\mathbb{Z}_p)$, existe um $n \in \mathbb{Z}_p$ tal que

$$Q = nP$$

Dizemos que n é o **Logaritmo Discreto Elíptico** de Q em relação a P, representamos $n = \log_P(Q)$. O Problema do Logaritmo Discreto Elíptico consiste em determinar n para cada ponto Q.

Como a operação de soma entre pontos de uma curva elíptica é consideravelmente mais trabalhosa que a multiplicação em $\mathbb{Z}_p$, determinar o logaritmo discreto elíptico sem conhecer os valores empregados no cálculo é ainda mais difícil que o Problema do Logaritmo Discreto em $\mathbb{Z}_p$.

O Problema do Logaritmo Discreto Elíptico está bem definido e $E(\mathbb{Z}_p)$ com a operação de adição entre dois pontos da curva é um grupo abeliano, logo, os resultados do capítulo 2 são válidos também para esta estrutura. Vejamos como os protocolos estudados naquele capítulo podem ser empregados com curvas elípticas.

Capítulo 4

CRIPTOGRAFIA COM CURVAS ELÍPTICAS

Para implementar um criptossistema baseado em curvas elípticas, é necessário fazer algumas mudanças nos protocolos estudados no capítulo 2 para adaptá-los à estrutura de curvas elípticas. Por exemplo, a equação da curva é um dado necessário ao processo de encriptação. Vejamos as mudanças realizadas.

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

Voltemos para o caso em que Alice e Bob desejam criar e compartilhar uma chave de codificação segura. No caso do protocolo Diffie-Hellman (ver seção 2.1), além do primo p e do gerador P, a equação da curva $E(\mathbb{Z}_p)$ também é um dado público, pois Alice e Bob precisam calcular os pontos empregando a mesma curva. O processo ocorre como segue:

1. Alice e Bob escolhem um primo p, uma curva $E(\mathbb{Z}_p)$ de equação $y^2 = x^3 + Ax + B$, com $4A^3 + 27B^2 \neq 0$, e um ponto $P \in E(\mathbb{Z}_p)$ gerador do grupo.

2. Alice escolhe um inteiro secreto $n_A \in \mathbb{Z}_p$, calcula $Q_A = n_A P$ e envia Q_A para Bob.

3. Bob escolhe um inteiro secreto $n_B \in \mathbb{Z}_p$, calcula $Q_B = n_B P$ e envia Q_B para Alice.

4. Alice calcula $R_A = n_A Q_B$

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

5. Bob calcula $R_B = n_B Q_A$

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

6. A chave secreta é $R_{AB} = R_A = R_B$

Como se pode ver, o procedimento para criar e compartilhar a chave secreta é o mesmo. A comunicação pode, então, ser realizada utilizando um criptossistema qualquer. Caso Carlos, um intruso, consiga interceptar a comunicação, deverá calcular o logaritmo discreto elíptico de Q_A e Q_B para obter os dados originais, o que e inviável.

4.2 Criptossistema ElGamal aplicado a curvas elípticas sobre $\mathbb{Z}_p$

Quando abordamos o criptossistema de chave pública ElGamal na seção 2.2, definimos o mesmo para o grupo multiplicativo $\mathbb{Z}_p$. No entanto, o ElGamal pode ser generalizado para um grupo cíclico finito qualquer. Voltemos para o caso de Alice e Bob.

Novamente, o primo p, a curva $E(\mathbb{Z}_p)$ de 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 de conhecimento público. Antes de iniciar o processo de encriptação, Bob, que deseja enviar uma mensagem codificada a Alice, deve transformar sua mensagem M em um ponto $P_M \in E(\mathbb{Z}_p)$[1]. Feito isto, pode-se iniciar a codificação.

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

2. Bob escolhe um inteiro aleatório k e calcula

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

[1] no caso de a mensagem ser um texto, normalmente se utiliza a tabela ASCII para converter em um número inteiro, ver figura 2.1

3. Bob envia para Alice o par de pontos (R, S)

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

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

O procedimento para transformar uma mensagem M em um ponto $P_M \in E(\mathbb{Z}_p)$ pode ser feito de várias maneiras, como por exemplo convertendo a mensagem para um inteiro empregando a tabela ASCII (figura 2.1) e, em seguida, separando este inteiro em duas coordenadas de um ponto, de tal forma que este ponto pertença à curva $E(\mathbb{Z}_p)$. Nos casos em que o ponto gerado por esta operação não pertence à curva, usualmente acrescenta-se zero, ou outro algarismo acordado entre as partes, até que as coordenadas encontradas formem um ponto de $E(\mathbb{Z}_p)$. Vejamos um exemplo:

Exemplo 4.1. *Considere a curva $E(\mathbb{Z}_{23})$ de equação $y^2 = x^3+9x+17$ e o ponto $P = (16, 5)$ gerador de $E(\mathbb{Z}_{23})$ com a operação de soma entre dois pontos. Transforme a mensagem M = MÁ em um ponto P_M da curva.*

Solução

Para tornar mais didático, utilizaremos a tabela abaixo em que cada letra, a partir de A, recebe um valor sequencial iniciado em 1.

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		

Figura 4.1: Tabela de correspondência letra-valor

Neste caso, temos que a mensagem M = MÁ, em termos numéricos, corresponde ao inteiro 1301 pois, pela tabela anterior, M = 13 e A = 01. Desmembrando este inteiro em duas coordenadas, encontramos o ponto $(13, 1)$, vejamos se este ponto pertence à curva:

$$y^2 = 1^2 = 1$$

$$x^3 + 9x + 17 = 13^3 + 9.13 + 17 = 2331 \equiv 8 \mod 23$$

Logo, $(13, 1) \notin E(\mathbb{Z}_{23})$, pois $1 \neq 8$. Devemos, então, fazer alguma modificação nas coordenadas do ponto. Vamos acrescentar o algarismo zero na ordenada do ponto encontrado, gerando o novo ponto $(13, 10)$, e vejamos se o mesmo pertence à curva.

$$y^2 = 10^2 = 100 \equiv 8 \mod 23$$

Portanto, a mensagem M é transformada no ponto $P_M = (13, 10)$ e está pronta para ser codificada.

□

Utilizando a mensagem e a curva do exemplo 4.1, vejamos como funciona o criptossistema ElGamal aplicado a curvas elípticas com um exemplo prático.

Exemplo 4.2. *Suponha que Bob deseja enviar a mensagem $M = MÁ$ para Alice empregando o primo, a curva e o ponto gerador do exemplo 4.1. Faça a codificação e decodificação da mensagem M utilizando o criptossistema ElGamal.*

Solução:

Como vimos no exemplo 4.1, $P_M = (13, 10)$. Vejamos os passos do ElGamal:

1. Suponhamos que Alice escolha $n_A = 4$. Temos:

$$P = (16, 5)$$

$$2P = (20, 20)$$

$$3P = (14, 14)$$

$$4P = (19, 20) = Q_A$$

2. Alice envia $(19, 20)$ para Bob.

3. Suponhamos que Bob escolha $k = 2$, temos

$$R = 2P = (20, 20)$$

$$S = P_M + 2.(19, 20) = (13, 10) + (12, 17) = (1, 21)$$

4. A mensagem codificada é formada pelos pontos $(20, 20)$ e $(1, 21)$, nesta ordem.

   Para decodificar a mensagem, basta Alice calcular

$$S - n_A R = (1, 21) - 4.(20, 20) = (1, 21) - (12, 17) =$$

$$= (1, 21) + (12, -17) = (1, 21) + (12, 6) = (13, 10) = P_M$$

   Portanto, Alice consegue ler a mensagem.

□

Capítulo 5

SUGESTÕES DE ATIVIDADES PARA O ENSINO MÉDIO

Neste capítulo sugerimos algumas maneiras de o professor de matemática empregar a temática deste trabalho como ponto de partida ou tema motivador para atividades no ensino médio. Não se pretende que o professor aplique diretamente o conteúdo de curvas elípticas em sala de aula, mas sim que o tema geral **Segurança da Informação** seja um norte na elaboração de sequências didáticas, haja visto que, de acordo com a Lei de Diretrizes e Bases da Educação Nacional - LDB, uma das finalidades do ensino médio é "a compreensão dos fundamentos científico-tecnológicos dos processos produtivos, relacionando a teoria com a prática no ensino de cada disciplina"(BRASIL, Lei 9394/96, Art. 35, IV)[1]. A atividade da seção 5.1 é direcionada para turmas do 1º ano do ensino médio, enquanto as demais atividades propostas neste capítulo são direcionadas para o 3º ano do ensino médio. Vejamos as atividades.

5.1 Noção Geral de Criptografia

Esta atividade objetiva propiciar um primeiro contato com a ideia de informação criptografada. É importante que o professor conceitue criptografia e mostre um esquema geral de funcionamento da mesma, conforme a figura a seguir.

Figura 5.1: Esquema geral de criptografia

O professor pode, também, mostrar o exemplo 2.3 para os alunos, sem entrar em detalhes quanto às operações realizadas, ou até mesmo preparar um exemplo de acordo com a atividade proposta a seguir. É importante que os alunos vejam pelo menos um exemplo de uma mensagem criptografada, para que possam observar na prática que, após o processo de encriptação, a mensagem se torna ilegível.

Recomenda-se que, neste momento, o professor não entre em detalhes quanto à diferença entre chaves secretas e públicas. Conforme vimos na definição 1.3.2, um criptossistema precisa de uma função de codificação e de sua função inversa, para decodificação. Nesta atividade, empregaremos função afim tanto para codificação quanto decodificação, uma vez que o aluno que já estudou este conteúdo está familiarizado a calcular imagens de valores específicos e determinar a função inversa. É recomendável, ainda, o uso de calculadora durante a realização da atividade.

Ações Didáticas

Separa-se a turma em grupos de até 4 alunos, para que todos possam participar ativamente. Para esta atividade, recomenda-se utilizar a tabela da figura 5.2, pois desta forma elimina-se números iniciados com algarismo 0. Entrega-se uma cópia desta tabela para cada grupo, orientando-os sobre como converter uma mensagem de texto em um número inteiro.

Letra	Valor	Letra	Valor	Letra	Valor
A	11	J	20	S	29
B	12	K	21	T	30
C	13	L	22	U	31
D	14	M	23	V	32
E	15	N	24	W	33
F	16	O	25	X	34
G	17	P	26	Y	35
H	18	Q	27	Z	36
I	19	R	28		

Figura 5.2: Tabela de correspondência letra-valor adaptada

Por exemplo, para converter a mensagem "MATEMÁTICA É LEGAL", deve-se primeiramente, para efeitos de simplificação, ignorar os espaços entre as palavras e acentuação, resultando em "MATEMATICAELEGAL". Em seguida, cada letra deve ser convertida conforme a tabela 5.2, resultando no inteiro

$$231130152311301913111522151711 22$$

Devido a limitações do visor da calculadora, o inteiro acima deverá ser separado em blocos. Recomenda-se deixar os alunos livres para fazer a separação da forma que acharem melhor. Uma maneira seria

$$231130 \quad 152311 \quad 301913 \quad 111522 \quad 1517 \quad 1122$$

É necessário explicar aos alunos que cada inteiro obtido a partir da separação da mensagem original é um elemento do domínio para o qual calcularemos a imagem via função de codificação. Neste momento, deve-se escolher qual será a função afim utilizada para codificação. Cada grupo receberá uma função diferente, fica a critério do professor determinar se cada um dos grupos terá liberdade para escolher a função empregada ou se o professor fornecerá as funções. Como exemplo, vamos utilizar a função f definida como segue:[1]

$$f : \mathbb{N} \to \mathbb{Z}$$

[1]Observe que o domínio da função é natural, mas, dependendo da função utilizada, a imagem pode ser um número negativo. Portanto, utilizaremos $\mathbb{Z}$ como contradomínio. É interessante aproveitar o momento para indagar os alunos quanto ao domínio e contradomínio da função.

$$x \mapsto 2x - 1$$

Aplicando a função a cada bloco de mensagem, temos:

$$f(231130) = 2.231130 - 1 = 462259$$

$$f(152311) = 2.152311 - 1 = 304621$$

$$f(301913) = 2.301913 - 1 = 603825$$

$$f(111522) = 2.111522 - 1 = 223043$$

$$f(1517) = 2.1517 - 1 = 3033$$

$$f(1122) = 2.1122 - 1 = 2243$$

Portanto, a mensagem criptografada é

$$462259 \quad 304621 \quad 603825 \quad 223043 \quad 3033 \quad 2243$$

Neste momento, o professor deverá trocar as mensagens criptografadas entre os grupos. Cada grupo deverá receber a mensagem criptografa e a função de codificação empregada. O grupo deverá, então, determinar a inversa f^{-1} da função recebida e aplicá-la a cada bloco de mensagem criptografada. No nosso exemplo, temos que $f^{-1}(y) = \dfrac{y+1}{2}$. Vejamos:

$$f^{-1}(462259) = \frac{462259+1}{2} = \frac{462260}{2} = 231130$$
$$f^{-1}(304621) = \frac{304621+1}{2} = \frac{304622}{2} = 152311$$
$$f^{-1}(603825) = \frac{603825+1}{2} = \frac{603826}{2} = 301913$$
$$f^{-1}(223043) = \frac{223043+1}{2} = \frac{223044}{2} = 111522$$
$$f^{-1}(3033) = \frac{3033+1}{2} = \frac{3034}{2} = 1517$$
$$f^{-1}(2243) = \frac{2243+1}{2} = \frac{2244}{2} = 1122$$

Desta forma, retornamos para a mensagem original. Basta, então, substituir cada bloco de dois dígitos por uma letra conforme a tabela da figura 5.2.

5.2 Determinar interseções entre uma reta e uma curva

Com esta atividade, pretende-se aplicar os conhecimentos dos alunos em conteúdos que envolvam determinar se um ponto pertence a uma curva, determinar a equação de uma reta e compreender as interseções entre duas curvas como sendo as soluções de um sistema de equações. É desejável que a atividade seja realizada em dupla, para verificação dos cálculos. Cada dupla deverá receber cópias impressas dos gráficos das curvas para manipulação.

Ações Didáticas

Para realizar esta atividade, deve-se, primeiramente, familiarizar o aluno com a ideia de ponto pertencente a uma curva, iniciando com curvas simples, como uma parábola. Observe o exemplo:

Exemplo 5.1. *Verifique se os pontos* $A = (1, 4)$ *e* $B = (2, -3)$ *pertencem à parábola* $y = x^2 - 4x + 1$

Solução:

Vejamos, primeiramente, o ponto A. Substituindo as coordenadas do ponto na equação da parábola, temos:

$$x^2 - 4x + 1 = 1^2 - 4.1 + 1 = 1 - 4 + 1 = -2$$

mas $y = 4$, como $-2 \neq 4$, A não pertence à parábola. Vejamos o ponto B:

$$x^2 - 4x + 1 = 2^2 - 4.2 + 1 = 4 - 8 + 1 = -3$$

Como $y = -3$, temos que B pertence à parábola

□

Após a familiarização, deve-se mostrar aos alunos o gráfico de uma curva elíptica, como a curva do exemplo 3.1, de equação $y^2 = x^3 - 2x + 2$, e pedir aos alunos que verifiquem se os pontos $C = (1, -1)$ e $D = (3, 4)$ pertencem à curva. Espera-se que os alunos respondam que apenas o ponto C pertence à curva. O professor deve perguntar qual o outro ponto da curva cuja coordenada $x = 1$ e quais os pontos cuja coordenada $x = 3$. Deve-se aproveitar esta oportunidade para explicar que a curva é simétrica em relação ao eixo horizontal.

Mostre, agora, a curva do exemplo 3.2, de equação $y^2 = x^3 - 4x + 3$, e peça que os alunos verifiquem que os pontos $(1, 0)$ e $(2, \sqrt{3})$ pertencem à curva. Alunos que já estudaram Geometria Analítica no ensino médio devem estar habituados a determinar a equação de uma reta que passa por dois pontos. Solicite que os alunos determinem a equação da reta que passa pelos pontos citados, o resultado deve ser

$$y = \sqrt{3}x - \sqrt{3}$$

.

Espera-se que os alunos percebam, a partir do gráfico, que a reta e a curva intersectam-se em três pontos, sendo que $(1, 0)$ e $(2, \sqrt{3})$ são dois pontos de interseção. Resta, portanto, determinar o terceiro ponto. Mostre para os alunos que, para encontrar este terceiro ponto, basta resolver o sistema de equações

$$\begin{cases} y^2 = x^3 - 4x + 3 \\ y = \sqrt{3}x - \sqrt{3} \end{cases}$$

Substituindo a segunda equação na primeira, obtemos:

$$(\sqrt{3}x - \sqrt{3})^2 = x^3 - 4x + 3$$

$$3x^2 - 6x + 3 = x^3 - 4x + 3$$

$$x^3 - 3x^2 + 2x = 0 \tag{5.1}$$

No ensino médio os alunos ainda não resolvem equações cúbicas, no entanto, a equação (5.1) é de fácil resolução. Colocando x em evidência, temos:

$$x(x^2 - 3x + 2) = 0$$

O que implica dizer que $x_1 = 0$ é uma raiz da equação. Para determinar as demais raízes, basta resolver a equação do segundo grau $x^2 - 3x + 2 = 0$, de onde obtemos $x_2 = 1$ e $x_3 = 2$, o que já sabíamos. Portanto, o terceiro ponto de interseção entre a reta e a curva elíptica é o ponto tal que $x = 0$, ou seja,

$$y = \sqrt{3}.0 - \sqrt{3} = -\sqrt{3}$$

.

O ponto procurado é $(0, -\sqrt{3})$

O professor pode aproveitar a oportunidade e destacar que, como a curva é simétrica em relação ao eixo horizontal, a reflexão deste ponto em relação ao referido eixo também pertence à curva. Peça que os alunos verifiquem que o ponto $(0, \sqrt{3})$ pertence à curva em questão. Alternativamente, o professor pode apresentar a definição 3.2.1 para o caso em que $P \neq Q$ e pedir que os alunos façam a verificação fazendo $P = (1, 0)$ e $Q = (2, \sqrt{3})$. É importante ressaltar para os alunos que, na definição 3.2.1, m é o coeficiente angular da reta entre P e Q. Uma outra forma de verificação de resultados nesta atividade é a utilização de softwares como o Geogebra.

5.3 Múltiplos de Pontos de Curvas sobre $\mathbb{Z}_p$

Para realizar esta atividade, os alunos deverão retomar a noção de resto de divisão inteira e trabalharão implicitamente com a ideia de congruência. Também será necessário fazer uma breve introdução à Aritmética Modular. Para facilitar a compreensão, pode-se definir o conjunto $\mathbb{Z}_p$, com p primo, da seguinte maneira:

$$\mathbb{Z}_p = \{x \in \mathbb{Z}_+ | x < p\}$$

Deve-se mostrar aos alunos que qualquer inteiro n possui um valor equivalente no conjunto $\mathbb{Z}_p$, bastando apenas calcular o resto da divisão de n por p. É interessante que o professor utilize a divisão inteira vista no teorema 1.2, ou seja, $n = pq + r$, sendo r o resto.

Por exemplo, $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Temos que, para $\mathbb{Z}_7$, 29 equivale a 1, pois $29 = 7.4 + 1$, logo, o resto da divisão de 29 por 7 é igual a 1. Em seguida, deve-se mostrar aos alunos como resolver equações em $\mathbb{Z}_p$. Vejamos um exemplo.

Exemplo 5.2. *Considere o conjunto $\mathbb{Z}_5$. Determine o valor de x na equação $3x = 4$.*

Solução:

Os possíveis valores de x são os elementos de $\mathbb{Z}_5$, ou seja:

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

Façamos a verificação para cada valor por tentativa e erro.

$$x = 0 \Longrightarrow 3.0 = 5.0 + 0 \text{ e } 0 \neq 4$$
$$x = 1 \Longrightarrow 3.1 = 5.0 + 3 \text{ e } 3 \neq 4$$
$$x = 2 \Longrightarrow 3.2 = 6 = 5.1 + 1 \text{ e } 1 \neq 4$$
$$x = 3 \Longrightarrow 3.3 = 9 = 5.1 + 4 \text{ e } 4 = 4$$

Portanto, temos $x = 3$.

□

Ações Didáticas

A partir do momento em que a turma conseguir resolver equações como a do exemplo 5.2, a atividade pode ser aplicada. Inicialmente, o professor deve introduzir a definição 3.2.1 e apresentar alguns exemplos de soma, certificando-se de que os alunos compreendam que o ponto O é o elemento neutro da operação. Podem ser utilizadas algumas das somas do exemplo 3.7, para habituá-los à operação.

Quando os alunos estiverem familiarizados, apresente a curva do exemplo 3.5, de equação $y^2 = x^3 - x + 3$ sobre $\mathbb{Z}_{11}$, mostrando todos os pontos da curva, a saber,

$$(0,5) \quad (0,6) \quad (1,5) \quad (1,6) \quad (2,3) \quad (2,8) \quad (3,3) \quad (3,7)$$
$$(6,2) \quad (6,9) \quad (7,3) \quad (7,8) \quad (8,1) \quad (8,10) \quad (10,5) \quad (10,6)$$

Solicite que os alunos escolham um ponto P qualquer e calculem o ponto $2P$. Em seguida, que façam um mesmo para um ponto Q qualquer, diferente de P, e determinem $2Q$. Após isto, proponha os seguintes questionamentos:

I - $2P$ pertence à curva?

II - $2Q$ pertence à curva?

- Calcule $P + Q$ e então calcule $2(P + Q)$
- Calcule $2P + 2Q$

III - Qual a relação entre $2(P + Q)$ e $2P + 2Q$?

IV - Se fizermos $3(P+Q)$ e $3P+3Q$ esta relação se mantém?

V - Calcule $2(2P)$ e $4P$. Qual a relação entre estes pontos?

O aluno deverá ser capaz de deduzir que nos itens III, IV e V acima os pontos em questão são iguais e, com isto, concluir que a multiplicação por escalar para um ponto da curva goza das propriedades associativa, comutativa, distributiva e pode considerar 1 como elemento neutro.

Voltemos, agora, para o exemplo 3.7, com $y^2 = x^3 + 2x - 1$ sobre $\mathbb{Z}_{13}$. Mostre para os alunos todos os múltiplos do ponto $P = (5, 2)$.

$$1P = P = (5, 2)$$
$$2P = P + P = (5, 2) + (5, 2) = (12, 3)$$
$$3P = 2P + P = (12, 3) + (5, 2) = (0, 8)$$
$$4P = 3P + P = (0, 8) + (5, 2) = (11, 0)$$
$$5P = 4P + P = (11, 0) + (5, 2) = (0, 5)$$
$$6P = 5P + P = (0, 5) + (5, 2) = (12, 10)$$
$$7P = 6P + P = (12, 10) + (5, 2) = (5, 11)$$
$$8P = 7P + P = (5, 11) + (5, 2) = O$$

É importante ressaltar que, para este ponto, tem-se que $8P = O$, deste modo, temos, por exemplo, que

$$13P = 8P + 5P = O + 5P = (0, 5)$$

ou ainda

$$37P = 4.8P + 5P = 4O + 5P = O + 5P = 5P = (0, 5)$$

Proponha o seguinte desafio para os alunos: considerando $P = (5, 2)$, determine o ponto $1500P$.

Uma maneira de resolver é empregando a decomposição

$$1500P = 187.8P + 4P = 187O + 4P = O + 4P = 4P = (11, 0)$$

Proponha que os alunos calculem $3000P$. Espera-se que os mesmos encontrem facilmente o resultado

$$3000P = 2.1500P = 2.4P = 8P = O$$

Deste modo, pode-se determinar qualquer múltiplo de P a partir de decomposições. Proponha que os alunos façam o mesmo escolhendo algum outro ponto da curva.

5.4 Simulação do Criptossistema ElGamal aplicado a curvas elípticas

Para aplicar esta atividade, é necessário que a turma já tenha realizado a atividade 5.3 anteriormente. Sugerimos que, antes de aplicar a atividade, seja feita um leitura atenta da seção 4.2 pelo professor.

Ações Didáticas

O professor deve separar a turma em várias duplas. Um aluno será o emissor e o outro será o receptor da mensagem criptografada. Para esta atividade utilizaremos a curva do exemplo 4.1, de equação $y^2 = x^3 + 9x + 17$ sobre $\mathbb{Z}_{23}$, considerando o ponto $P = (16, 5)$ como gerador. Abaixo, temos o mapeamento de todos os pontos desta curva:

$$(1,2) \quad (1,21) \quad (3,5) \quad (3,18) \quad (4,5) \quad (4,18)$$

$$(5,7) \quad (5,16) \quad (7,3) \quad (7,20) \quad (8,7) \quad (8,16)$$

$$(10,7) \quad (10,16) \quad (12,6) \quad (12,17) \quad (13,10) \quad (13,13)$$

$$(14,9) \quad (14,14) \quad (15,10) \quad (15,13) \quad (17,0) \quad (18,10)$$

$$(18,13) \quad (19,3) \quad (19,20) \quad (20,3) \quad (20,20)$$

Solicite que cada aluno emissor secretamente escolha um dentre os pontos do mapeamento e não informe para o colega de dupla. Os alunos executarão o passo a passo do criptossistema ElGamal, seguindo as orientações do professor. Verifique se o ponto escolhido pelo aluno emissor é o mesmo obtido pelo aluno receptor. Em seguida, deve-se repetir a atividade, trocando os papéis de cada aluno. o emissor passa a ser receptor e vice versa.

CONSIDERAÇÕES FINAIS

Neste trabalho estudamos um método de criptografia que envolve curvas elípticas, cuja segurança é garantida pela dificuldade de solução do problema do logaritmo discreto. Vimos que determinar o logaritmo discreto, para primos com grande quantidade de algarismos, é um procedimento inviável, pois demanda um tempo considerável para se encontrar a solução. Com base nisto, mostramos dois modelos de criptografia que se utilizam da dificuldade descrita anteriormente para proporcionar segurança na transmissão de dados.

Mostramos que uma curva elíptica definida sobre um corpo $\mathbb{Z}_p$, munida da operação de soma entre dois pontos da curva, é um grupo abeliano. Desta forma, o problema do logaritmo discreto pode ser adaptado a esta estrutura e, deste modo, podemos aplicar os métodos de criptografia estudados, realizando as devidas adaptações.

Sugerimos algumas atividades para aplicação em turmas do ensino médio baseadas no tema deste trabalho. Com o crescimento do acesso a tecnologias da informação, observa-se maior interesse dos discentes por assuntos relacionados a esta área. Ao utilizar celulares com aplicativos de troca de mensagens e outros que requerem sigilo da informação, indiretamente se está utilizando algum sistema de criptografia. Pode-se utilizar este fato como ponto de partida para introduzir o tema segurança da informação como motivador para a realização das atividades propostas neste trabalho. Com isto, objetivamos despertar o interesse do aluno pela matemática por trás da prática em assuntos relacionados a tecnologia da informação

Ainda há muito a ser estudado sobre o tema e muitas abordagens possíveis. Pretende-se, com este trabalho, contribuir para o enriquecimento da bibliografia sobre o tema em língua portuguesa, que ainda é escassa.

Referências Bibliográficas

[1] BRASIL, LEI 9394 de 20/12/1996. **Lei de Diretrizes e Bases da Educação Nacional**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9394.htm>. Acesso em: 24 de janeiro de 2015.

[2] CORREIA JUNIOR, Sergio dos Santos. **Criptografia via curvas elípticas**. 2013. 87 f. Dissertação (Mestrado Profissional em Matemática - PROFMAT) - Universidade Federal do Estado do Rio de Janeiro - UNIRIO. Disponível em: <http://www2.unirio.br/unirio/ccet/profmat/tcc/2011/TCCSergioCorreia.pdf>. Acesso em: 23 de agosto de 2015.

[3] DELGADO, J., FRENSEL, K., CRISSAFF, L. **Geometria Analítica**. SBM, 2014 (Coleção PROFMAT).

[4] DIFFIE, W. and HELLMAN, M.E. New directions in criptography. **IEEE Transactions on Information Theory**. Vol. 22, Nº 6, Pág. 644-654, 1976.

[5] GONÇALVES, Adilson. **Introdução à Álgebra**. Rio de Janeiro: IMPA, 2008

[6] HERSTEIN, I. N. **Topics in Algebra**. Chicago: Blaisdell Publishing Company, 1964.

[7] LANDAU, Edmund. **Teoria Elementar dos Números**. Coleção Clássicos da Matemática. 1ª edição. Rio de Janeiro: Ciência Moderna, 2002.

[8] MILLIES, César Polcino & COELHO, Sônia Pitta. **Números. Uma Introdução à Matemática**. 3ª edição. São Paulo: Edusp, 2001.

[9] SAEKI, Mugino. **Elliptic curve cryptosystems**. 1997. 82 f. Dissertação (Master of Science in Computer Science) - School of Computer Sciences, McGill University, Mon-

treal. Disponível em <http://www.cs.mcgill.ca/ crepeau/PDF/memoire-mugino.pdf>. Acesso em: 23 de agosto de 2015.

[10] SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. Coleção Matemática Universitária. Rio de Janeiro: IMPA, 1998.

[11] SILVERMAN, Joseph H. **The Arithmetic of Elliptic Curves.**. Graduate Texts in Mathematics. 2nd edition. San Francisco: Springer, 2009.

[12] SIPSER, Michael. **Introdução à Teoria da Computação**. São Paulo: Thomson, 2007.

[13] STALLINGS, William. **Criptografia e Segurança de Redes: princípios e práticas**. 4ª edição. São Paulo: Pearson Prentice Hall, 2008.

[14] STINSON, Douglas R. **Criptography: theory and practice**. 3rd edition. Boca Raton/Florida: Chapman & Hall, 2006.

[15] TERADA, Routo. **Segurança de Dados: criptografia em redes de computador**. São Paulo: Edgar Blücher, 2000.

[16] WASHINGTON, Lawrence C. **Elliptic Curves: number theory and criptography**. 2nd edition. Boca Raton: Chapman & Hall, 2008.

Apêndice A – Programa para calcular o logaritmo discreto

Para calcular o logaritmo discreto nos exemplos do texto, elaboramos um programa na linguagem de programação C++ que, dados o primo p, o gerador g de $\mathbb{Z}_p$ e o inteiro para o qual desejamos calcular o logaritmo discreto, retorna o valor do logaritmo. Para isto, o programa testa todos os valores possíveis, iniciando em 1, até encontrar o resultado.

```
#include <iostream>
#include <cmath>
using namespace std;

int resto;

int main()
{
      int primo; //primo p
      int contador=0; //controla o expoente
      int gerador; //gerador de Zp
      int logaritmo; //valor para o qual sera calculado o logaritmo
      cout « "Informe o numero primo p:  "; //exibicao na tela
      cin » primo; //leitura do valor informado pelo usuario
      cout « "Informe o gerador de Z"« primo « ":  ";
      cin » gerador;
      cout « "Informe o valor para calcular o logaritmo:  ";
```

```
      cin » logaritmo;
      resto=primo+1; //p+1 congruente a 1 mod p
      while (resto != logaritmo) //enquanto o resto nao for o esperado
      {
            contador++;
            resto=(gerador*resto)%primo;
            cout « contador-1 « "nao e a resposta" « endl;
      }
      endl;
      cout « "O resultado e "« contador « endl;
}
```

Anexo A – Demonstração do Teorema 1.1: Teorema Fundamental da Aritmética

Apresentamos uma demonstração do Teorema 1.1 retirada de SANTOS [10], página 9.

Teorema 1.1 (Teorema Fundamental da Aritmética). *Todo número inteiro positivo maior que* 1 *pode ser escrito de maneira única como o produto de números primos, a menos da ordem dos fatores.*

Demonstração:

Seja n um número inteiro. Se n é primo, não há nada a ser demonstrado. Suponhamos, pois, n composto. Seja p_1, com $p_1 > 1$, o menor dos divisores positivos de n. Afirmamos de que p_1 é primo. Isto é verdade, pois, caso contrário, existiria p, com $1 < p < p_1$, tal que $p|n$, contradizendo a escolha de p_1. Logo, $n = p_1 n_1$.

Se n_1 for primo, a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 p_2 n_2$.

Repetindo este procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, \ldots, n_r$. Como todos eles são inteiros maiores do que 1, este processo deve terminar. Como os primos na sequência $p_1, p_2, \ldots, p_k$ não são, necessariamente, distintos, n terá, em geral, a forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

Para mostramos a unicidade usamos indução em n. Para $n = 2$ a afirmação é

verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_r$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 q_2 \dots q_r$, ele divide pelo menos um dos fatores q_j. Sem perda de generalidade, podemos supor que $p_1 | q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo, $n/p_1 = p2 \dots p_s = q_2 \dots q_r$. Como $1 < n/p_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 \dots p_s$ e $q_1 q_2 \dots q_r$ são iguais.

□

Anexo B – Demonstração do Teorema 1.3: Pequeno Teorema de Fermat

Apresentamos uma demonstração do Teorema 1.3 retirada de SANTOS [10], página 41.

Teorema 1.3 (Pequeno Teorema de Fermat). *Sejam p primo e a um inteiro. Se $p \nmid a$, então* $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração:

Sabemos que o conjunto formado pelos p números $0, 1, 2, \ldots, p-1$ constitui um sistema completo de resíduos módulo p (ver definição 1.1.5). Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, 2, \ldots, p-1\}$. Vamos, agora, considerar os números $a, 2a, 3a, \ldots, (p-1)a$. Como $\text{mdc}(a, p) = 1$, nenhum destes números ia, $1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak \pmod{p}$ implica $j \equiv k \pmod{p}$ e isto só é possível se $j = k$, uma vez que ambos j e k são positivos e menores do que p. Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo p e não-divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, \ldots, p-1$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a(2a)(3a)\ldots(p-1)a \equiv 1.2.3\ldots(p-1) \ (\text{ mod } p)$$

ou seja, $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Mas, como $\text{mdc}((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

$$a^{p-1} \equiv 1 \ (\text{ mod } p),$$

finalizando, assim, a demonstração.

Anexo C – Demonstração do Teorema 1.5: Teorema de Euler

Apresentamos uma demonstração do Teorema 1.5 retirada de SANTOS [10], página 43.

Teorema 1.5 (Teorema de Euler). *Sejam* $a, m \in \mathbb{Z}$ *com* $m \geq 1$, *tais que* $\text{mdc}(a, m) = 1$, *então*

$$a^{\phi(m)} \equiv 1 \ (\text{mod } m)$$

Demonstração:

No teorema 1.4 mostramos que os elementos $ar_1, ar_2, \ldots, ar_{\phi(m)}$ constituem um sistema reduzido de resíduos módulo m se $\text{mdc}(a, m) = 1$ e $r_1, r_2, \ldots, r_{\phi(m)}$ for um sistema reduzido de resíduos módulo m. Isto significa que ar_i é congruente a exatamente um dos r_j, $1 \leq j \leq \phi(m)$, e portanto o produto dos ar_i deve ser congruente ao produto dos r_j módulo m, isto é,

$$ar_1.ar_2 \ldots ar_{\phi(m)} \equiv r_1.r_2 \ldots r_{\phi(m)} \ (\text{mod } m)$$

ou seja

$$a^{\phi(m)} r_1.r_2 \ldots r_{\phi(m)} \equiv r_1.r_2 \ldots r_{\phi(m)} (\text{mod } m)$$

Como para cada r_i, com $1 \leq r_i \leq \phi(m)$, temos $\text{mdc}(r_i, m) = 1$, podemos cancelar cada r_i em ambos os lados para obter $a^{\phi(m)} \equiv 1 \ (\text{mod } m)$

□