Instituto federal de Educação, Ciência e Tecnologia de Goiás

Câmpus Valparaíso

Licenciatura em Matemática

CURSO DE LICENCIATURA EM MATEMÁTICA

O USO DA ARITMÉTICA MODULAR NO DESENVOLVIMENTO DA CRIPTOGRAFIA RSA

JOEL PEREIRA DOS SANTOS

VALPARAÍSO DE GOIÁS

2023

TERMO DE AUTORIZAÇÃO PARA DISPONIBILIZAÇÃO NO REPOSITÓRIO DIGITAL DO IFG - ReDi IFG

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia de Goiás, a disponibilizar gratuitamente o documento no Repositório Digital (ReDi IFG), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IFG.

Identificação da Produção Técnico-Científica

[ ] Tese	[ ] Artigo Científico
[ ] Dissertação	[ ] Capítulo de Livro
[ ] Monografia – Especialização	[ ] Livro
[X] TCC - Graduação	[ ] Trabalho Apresentado em Evento
[ ] Produto Técnico e Educacional - Tipo: _____	

Nome Completo do Autor:
Matrícula:
Título do Trabalho:

Autorização - Marque uma das opções

1. (X) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso aberto);
2. ( ) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG somente após a data ___/___/_____ (Embargo);
3. ( ) Não autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso restrito).

Ao indicar a opção **2 ou 3**, marque a justificativa:

( ) O documento está sujeito a registro de patente.
( ) O documento pode vir a ser publicado como livro, capítulo de livro ou artigo.
( ) Outra justificativa: _____

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

i. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
ii. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia de Goiás os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
iii. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

gov.br Documento assinado digitalmente
JOEL PEREIRA DOS SANTOS
Data: 11/07/2024 19:12:51-0300
Verifique em https://validar.iti.gov.br

Valparaíso de Goiás, 10/07/2024.

_____
Assinatura do Autor e/ou Detentor dos Direitos Autorais

JOEL PEREIRA DOS SANTOS

O USO DA ARITMÉTICA MODULAR NO DESENVOLVIMENTO DA CRIPTOGRAFIA RSA

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática do Instituto Federal de Goiás - IFG - Câmpus Valparaíso, como requisito parcial para obtenção do título de Licenciado em Matemática.

Área de Concentração: Teoria dos Números

Orientador: Bruno de Paula Miranda

VALPARAÍSO DE GOIÁS

2023

Ficha catalográfica elaborada pelo bibliotecário Helio Lino Delfino (CRB-1/3031), com os dados fornecidos pelo(a) autor(a).

S237u

Santos, Joel Pereira dos.
O uso da aritmética modular no desenvolvimento da criptografia RSA./ Joel Pereira dos Santos.
– Valparaíso de Goiás: IFG, 2023.
45 f.

Orientador: Prof. Dr. Bruno de Paula Miranda.
TCC (Graduação - Licenciatura em Matemática) –
- Instituto Federal de Goiás – IFG, Câmpus Valparaíso de Goiás, 2023.

1. Aritmética modular - Matemática. 2. Criptografia RSA. I. Miranda, Bruno de Paula. II. Título.

CDD 510

Termo de Aprovação

JOEL PEREIRA DOS SANTOS

O USO DA ARITMÉTICA MODULAR NO DESENVOLVIMENTO DA CRIPTOGRAFIA RSA

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia de Goiás – Câmpus Valparaíso de Goiás, como parte dos requisitos para a obtenção do título de Licenciado em Matemática.

Monografia defendida e aprovada em 14 de dezembro de 2023 pela banca examinadora constituída pelos seguintes membros:

BANCA EXAMINADORA

Prof. Dr. Bruno de Paula Miranda
Presidente da banca / Orientador
Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Profa. Dra. Daiane Soares Veras
Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Prof. Dr. Yerko Contreras Rojas
Universidade Federal do Sul e Sudeste do Pará

Valparaíso de Goiás – GO

2023

Documento assinado eletronicamente por:

- **Daiane Soares Veras, PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 21/12/2023 13:27:42.
- **Bruno de Paula Miranda, PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 20/12/2023 17:44:35.

gov.br
Documento assinado digitalmente
YERKO CONTRERAS ROJAS
Data: 09/07/2024 17:23:16-0300
Verifique em https://validar.iti.gov.br

Este documento foi emitido pelo SUAP em 14/12/2023. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifg.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 490589
Código de Autenticação: 522fbc669c

Dedicatória

Dedico esse trabalho a meu Jesus Cristo, meu Deus, pois sem ele eu não poderia ter feito nada disso. Ele é quem me dá força em todos os momentos e está sempre comigo. Eu te amo, Jesus!!!

Agradecimentos

Agradeço primeiramente a Deus por me conceder a oportunidade de consumar um sonho que tenho desde criança, que é o de me tornar um professor de matemática, disciplina que amo.

Em seguida, agradeço minha família (isto é, meu pai José, minha mãe Eliete e meus irmãos Jonas e Ester), que sempre me deu apoio, tanto nos bons momentos como nos momentos em que eu pensei em desistir devido a algumas desilusões e decepções. Agradeço a todos os que estiveram e/ou estão em minha vida durante o período da faculdade e que me ajudaram neste percurso, em especial minha namorada atual Sara, meu amigo de infância Gabriel Duarte e meus amigos de faculdade Gabriel Lucas, Mikeias e Carlos, com quem eu caminhei em boa parte desta jornada.

Agradeço também a todos os professores que transmitiram os conhecimentos necessários da Matemática e da Licenciatura, especialmente aqueles com quem tive uma relação mais próxima. Em particular, agradeço ao meu orientador Bruno, que não só me orientou neste trabalho, como também em Iniciações científicas, além de ter me dado muitos conselhos.

Por fim, agradeço a todos que, de algum modo, puderam me ajudar nesta jornada. A todos meu "Muito Obrigado"!!!

Resumo

Este trabalho, intitulado *O uso da aritmética modular no desenvolvimento da Criptografia RSA*, tem como objetivo estudar os fundamentos por traz da Criptografia RSA, a saber, a aritmética modular, suas características e propriedades. Inicialmente, são estudadas algumas propriedades básicas dos números inteiros para, em seguida, definir a congruência entre dois inteiros dado um terceiro inteiro e apresentar suas propriedades básicas. Em sequência, o conceito de inverso módulo n é apresentado e conceituado, além de ser especificadas as suas propriedades e a sua condição de existência; além disso, também são estabelecidas as relações entre inversos e alguns teoremas bastante utilizados na Criptografia RSA, como o Teorema Chinês do Resto e o Pequeno Teorema de Fermat. Feito toda esta fundamentação teórica, a Criptografia RSA é apresentada e definida, além de mostrar como e por que a Criptografia RSA funciona, utilizando a congruência modular para tais finalidades; dentro disso, é apresentado um exemplo simples de codificação e decodificação na Criptografia RSA. Por fim, são feitas algumas considerações sobre a Criptografia RSA, sua efetividade e a dificuldade de uma pessoa não-autorizada fazer a decodificação de uma mensagem, isto é, quebrar o código, sem a posse das chaves privadas para decodificação.

Palavras-chave: Criptografia. Aritmética Modular. Inteiros. Inverso. Codificação. Decodificação.

Abstract

This work, entitled *The use of modular arithmetic in the development of RSA Cryptography*, aims to study the fundamentals behind RSA Cryptography, namely, modular arithmetic, your characteristics and properties. Initially, some basic properties of integers are studied to, then, to define the congruence between two integers given a third integer and present your basic properties. In sequence, the concept of inverse module n is presented and conceptualized, in addition to specifying your properties and condition of existence; Furthermore, relationships between inverses and some theorems widely used in RSA Cryptography are also established, such as the Chinese Remainder Theorem and Fermat's Little Theorem. Having done all this theoretical foundation, RSA Cryptography is presented and defined, in addition to showing how and why RSA Cryptography works, using modular congruence for such purposes; Within this, a simple example of coding and decoding in RSA Cryptography is presented. Finally, some considerations are made about RSA Encryption, y effectiveness and the difficulty for an unauthorized person to decode a message, that is, to break the code, without possession of the private keys for decryption.

Keywords: Cryptography. Modular Arithmetic. Integers. Inverse. Coding. Decoding.

Notações

$a \equiv b \mod n$: a é congruente a b módulo n

Sumário

Introdução

A criptografia é uma área de estudo que consiste em transmitir uma mensagem em forma de código de um emissor, que codificou a mensagem, para um receptor escolhido pelo emissor, que recebe a mensagem codificada e, por meio das ferramentas para código, decodifica-a para a sua forma original. Segundo Coutinho (2014) criptografia existe desde a antiguidade, sendo usada pelos romanos. Mais recentemente, com o advento da internet e da computação gráfica, foram desenvolvidos diversos métodos de criptografia para a proteção de dados, seja eles bancários, militares, econômicos ou até mesmo dados pessoais. Um desses métodos é a Criptografia RSA, que surgiu na década de 1970 no Massachussets Institute of Technology (MIT). A Criptografia RSA se utiliza de um ramo da Matemática denominado *Teoria dos Números*.

Neste trabalho, serão descritos e demonstrados alguns fundamentos da Aritmética Modular, que é uma das áreas da Teoria dos Números, bem como suas propriedades, características e peculiaridades, que serão de valia para a formalização, descrição e utilização da Criptografia RSA.

Inicialmente, no capítulo 1 serão descritos e fundamentados os aspectos mais básicos dos números inteiros que serão utilizados posteriormente.

No capítulo dois, os aspectos iniciais da Aritmética Modular serão apresentados e discutidos, isto é, a *Congruência Modular* será definida e suas propriedades básicas serão abordadas.

No Capítulo 3, um importante conceito relacionado a congruência modular será definido e discutido: o conceito de *Inverso*. Neste mesmo capítulo, serão discutidas algumas consequências relacionadas a existência de inverso, como o Teorema Chinês do Resto e o

Pequeno Teorema de Fermat (aqui chamado apenas de Teorema de Fermat).

Por fim, no Capítulo 4, a Criptografia RSA será apresentada e fundamentada, mostrando os processos de codificação e decodificação de uma mensagem dentro desse método de criptografia, com um exemplo básico. Neste mesmo capítulo, a funcionalidade do RSA será demonstrada.

Capítulo 1

Noções Básicas dos Números Inteiros

Para conhecer os algoritmos e processos envolvendo a Criptografia RSA, é necessário, antes, compreender as noções básicas relacionadas ao conjunto dos números inteiros (denotado por $\mathbb{Z}$), como múltiplos e divisores, primos, compostos e fatoração de um número inteiro por números primos. Cada um destes aspectos será visto a seguir.

1.1 Múltiplos e Divisores

Os números inteiros possuem propriedades interessantes relacionadas ao Algoritmo da Divisão Euclidiana, que diz que, dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem únicos inteiros $q, r \in \mathbb{Z}$ com

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

Como é sabido desde o início dos estudos, um número inteiro pode ou não ser dividido por um outro número inteiro. Assim:

Definição 1. Diz-se que b é um *divisor* de a, ou ainda, a é *múltiplo* de b quando existe um inteiro c tal que $a = bc$.

Uma informação importante é que o número c é chamado de *cofator* de b em a, isto é, c é o quociente da divisão de a por b quando essa divisão é exata, isto é, quando $r = 0$ no Algoritmo da Divisão Euclidiana. Como exemplo, o número 3 é divisor de 93, pois

$93 = 3 \cdot 31$. Da mesma forma, o número 31 também é um divisor de 93. Já o número 2 não é um divisor de 93, pois não existe um inteiro c tal que $93 = 2 \cdot c$. Naturalmente, fazendo $c = 1$, tem-se que todo número inteiro a divide a si mesmo. Analogamente, $-a$ também divide a. Usando raciocínio semelhante, tem-se que os números $+1$ e -1 dividem todo e qualquer número inteiro e, como consequência $+1$ e -1 são *fatores comuns*, isto é, divisores comuns, a dois ou mais inteiros. No caso de existir um inteiro b divisor de um inteiro a, e que seja diferente de ± 1 e $\pm a$, damos um nome especial para tal tipo de divisor.

Definição 2. Diz-se que b é um *divisor próprio* de a quando b divide a e $1 < b < a$.

Por meio desta definição, conclui-se que 1 e o próprio a não serão divisores próprios de a. Esta informação será importante para definições futuras.

Definição 3. Dois números a e b são *primos entre si* quando possuem apenas ± 1 como fator comum, isto é, quando apenas ± 1 são divisores comuns de a e b.

A partir da definição 1, temos a seguinte propriedade:

Propriedade dos Múltiplos. Sejam a, b, c e d números inteiros:

1. d divide 0 ;
2. se d divide a e b, então divide $a + b$;
3. se d divide a, então divide $a \cdot c$.

Demonstração. A parte 1 é fácil de verificar, pois a multiplicação de 0 por qualquer número inteiro é igual a 0, isto é, todo número inteiro é divisor de 0 .
Do item 2, tem-se que, se d divide a e b, então, pela definição 1:

$$a = d \cdot a' \text{ e } b = d \cdot b'$$

onde a' e b' são cofatores de, respectivamente, a e b. Ora, somando a e b

$$a + b = d \cdot a' + d \cdot b'$$
$$a + b = d \cdot (a' + b')$$

como é necessário demonstrar.

Do item 3 tem-se que, se d é divisor de a, então, por definição

$$a = d \cdot a'$$

e, multiplicando a igualdade acima por c

$$a \cdot c = (d \cdot a') \cdot c = d \cdot (a' \cdot c)$$

de modo que d divide $c \cdot a$

□

A partir das definições a seguir, é possível definir números primos e compostos, bem como apresentar algumas de suas propriedades; é o que será visto a seguir.

1.2 Primos e Compostos

Dentro da Criptografia RSA, um número ser primo ou composto é de significativa importância para codificar ou decodificar informações. Assim, é necessário definir estes dois conceitos, como será feito a seguir.

Definição 4. Um número inteiro $p > 1$ é dito *primo* quando seus únicos divisores são ± 1 e $\pm p$. Quando o número inteiro não é primo, diz-se que ele é um número *composto*.

Por meio da definição acima, os números 2, 3, 23 e 43 são primos, porem $68 = 2 \cdot 34$ não é primo. Note que o número 68 pode ser escrito como $68 = 2 \cdot 2 \cdot 17$, onde 2 e 17 são primos. Em geral, números inteiros compostos são produtos de potências de primos. Este resultado será mostrado mais adiante. Um exemplo menos trivial da definição acima é o exemplo a seguir:

Exemplo 1.2.1. Seja $n > 1 \in \mathbb{Z}$ e $n!$ o produto de todos os inteiros positivos menores ou iguais a n. Então os números consecutivos

$$n! + 2, n! + 3, ..., n! + (n - 1)$$

não são primos.

Demonstração. Ora,

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$$

de modo que

$$2 \leq k \leq n-1$$

são divisores próprios de $n!$.

Percebe-se que os números

$$n! + 2, n! + 3, ..., n! + (n-1)$$

podem ser escritos na forma $n! + k$, com $2 \leq k \leq (n-1)$. Pelo item 2 da Propriedade dos Múltiplos, descrita na seção anterior, como k divide tanto $n!$ como o próprio k, então tem-se que k divide também $n! + k$.

Portanto, os números $n!+2, n!+3, ..., n!+(n-1)$, escritos na forma $n!+k$, são compostos.

□

Note que o fatorial acima pode ser decomposto em produtos de números inteiros. Este processo, que ocorre não só com os fatoriais, mas também com os demais números inteiros, é chamado de *fatoração*, que será estudado a seguir.

1.3 Fatoração de Números Inteiros

O último passo antes de iniciar o estudo da aritmética modular é compreender a fatoração, suas características e propriedades. Começamos com a definição a seguir:

Definição 5. A *fatoração* é o processo de decomposição de um número inteiro em fatores também inteiros.

A técnica mais básica de fatoração é escolher um inteiro a e dividi-lo por um inteiro menor que a, obtendo um quociente; em seguida, deve-se dividir este quociente por um inteiro menor que ele; este processo é repetido até que o quociente final seja 1. Neste modelo mais básico existem diferentes formas de fatorá-lo. Por exemplo, tomando, $a = 40$

e escolhendo um divisor $d = 5$, temos $40 = 5 \cdot 8$; como 8 ainda pode ser divisível, temos que $8 = 4 \cdot 2$ e $40 = 5 \cdot 8 = 5 \cdot 4 \cdot 2$. Este processo continua até que não haja mais divisores para nenhum dos fatores. Ao fatorar o 40, caso fosse tomado um divisor aleatório para iniciar o processo, é possível ver que:

- 40 é divisível por 2, pois é par.
- 40 não é divisível por 3, pois a soma de seus algarismos não é um múltiplo de 3.
- 40 é divisível por 4, pois $4 \cdot 10 = 40$.
- 40 é divisível por 5, pois o número 40 termina em 0.
- 40 não é divisível por 6, pois $6 = 2 \cdot 3$ e 3 não divide 40 (relembre do item 2 da Propriedade dos Múltiplos).

Este processo se estenderia até o 39, o antecessor de 40.

Note que, usando como base o item 2 da Propriedade dos Múltiplos, como 3 não divide 40, nenhum outro múltiplo de 3 divide 40. Essa afirmação pode ser generalizada, para facilitar o processo acima, na proposição a seguir.

Proposição 1.1. *Se um inteiro k divide um inteiro m, que por sua vez divide outro inteiro n, então k divide n.*

Demonstração. Se k divide m, entao

$$m = k \cdot c, c \in \mathbb{Z} \tag{1.1}$$

Se m divide n, entao

$$n = m \cdot d, d \in \mathbb{Z} \tag{1.2}$$

Substituindo (1.1) em (1.2), temos

$$n = k \cdot c \cdot d = k(c \cdot d)$$

e, portanto, k divide n □

A proposição acima reduz o processo descrito à divisão de um número inteiro por números primos menores que ele. No caso do número 40, o processo se reduziria a dividir o 40 por números primos menores que 40. Caso não houvessem primos menores que 40 que o dividissem, seria certo afirmar que o número 40 é primo. Observe também que o processo começa, agora, dividindo o número 40 por 2, que é o menor primo positivo. Caso o 2 não dividisse 40, o próximo número a ser analisado seria o 3, que é o próximo primo. Em geral, como consequência desta proposição, todo número composto tem como menor divisor próprio um número primo.

O processo acima pode ser trabalhoso e difícil de ser aplicado para números inteiros com muitos algarismos. Mas este processo pode ser reduzido mais ainda, de acordo com a proposição adiante:

Proposição 1.2. *Se n for composto, o menor divisor próprio de n é menor ou igual a raiz quadrada de n*

Demonstração. Ora, se n é composto, então n possui como menor fator um primo p, de modo que

$$n = p \cdot c \tag{1.3}$$

Da igualdade (1.3), tem-se que c é também um fator de n, mas como p é o menor fator de n, então

$$c \geq p \tag{1.4}$$

de modo que (1.3) e (1.4) implica em

$$n = p \cdot c \geq p \cdot p = p^2$$

que é o mesmo que

$$p \leq \sqrt{n}$$

□

Isto significa que todos os números compostos são divisíveis por pelo menos um primo menor ou igual a sua raiz quadrada, de modo que o processo acima é reduzido a dividir o inteiro por primos menores que sua raiz quadrada. Caso não haja estes divisores, então o inteiro será primo. Note que, por meio deste processo, é possível decompor um número inteiro dividindo-o pelo menor primo possível, desde que o primo seja menor do que a raiz quadrada do número inteiro a ser dividido.

Veja o caso do número 40. O primeiro número primo é o 2, que divide o 40, obtendo o resultado igual a 20; este, por sua vez, é dividido por 2, com resultado igual a 10, que, por sua vez, é dividido por 2, com resultado igual a 5. Note que a raiz quadrado de 5 é um número aproximado ao 2, mas o 5 não é divisível por 2, sendo, assim, primo. Assim, pode-se reescrever o número 40 da seguinte forma:

$$40 = 20 \cdot 2 = 10 \cdot 2 \cdot 2 = 5 \cdot 2 \cdot 2 \cdot 2 \Rightarrow 40 = 5 \cdot 2^3$$

Generalizando o que foi feito com o número 40, todo número inteiro pode ser reescrito, de uma única forma, como produto de potências de números primos, como evidenciado pelo teorema a seguir:

Teorema 1.3 (Teorema da Fatoração Única)**.** *Dado um número inteiro positivo $n \geq 2$, pode-se reescrevê-lo, de modo único, na forma*

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

onde $p_1, ..., p_k$ são primos positivos e $e_1, ..., e_k$ são números inteiros positivos

Demonstração. O Teorema será provado em duas partes: a parte 1 demonstrará a decomposição de um número inteiro e a parte 2 mostrará a unicidade da fatoração.
Parte 1:

Seja n um inteiro positivo maior do que 1. Se n for primo, então seu único divisor diferente de 1 é ele mesmo: essa decomposição será chamada de decomposição trivial. Se n for composto, então existe p_1 como o menor fator primo de n, de modo que

$$n = p_1 \cdot c_1$$

Se c_1 for primo, então a decomposição é trivial, e o número n pode ser escrito como $n = p_1 c_1$. Se c_1 for composto, então, como visto na demonstração da Proposição 1.2, existe p_2 tal que $c_1 = p_2 c_2$. O processo se repetirá até cair numa decomposição trivial, isto é, até todos os divisores serem números primos.

Parte 2

A parte 2 será demonstrada por indução.

Seja n um número inteiro positivo e seja s o número de fatores primos da decomposição de n. Suponha que n tenha duas decomposições em primos, isto é, $n = p_1$ (de comprimento $s = 1$) e $n = q_1 q_2 \cdots q_m$ (de comprimento $s = m$). Assim, tem-se que

$$p_1 = q_1 q_2 \cdots q_m \tag{1.5}$$

de modo que q_1 divide p_1. Como q_1 é primo, tem-se que $p_1 = q_1$, de modo que, cancelando p_1 e q_1 da igualdade (1.5), temos

$$1 = q_2 \cdots q_m$$

o que é impossível, pois $q_2 \cdots q_m$ é um produto de números primos. Assim, todo inteiro com um único fator primo (isto é, $s = 1$) admite uma única decomposição.

Suponha agora que todo $n = p_1 p_2 \cdots p_k$, de comprimento $s = k$ (isto é, há k fatores primos), tenha admita uma única decomposição em primos. Será provado que todo número n_1, de comprimento $k + 1$, tem apenas uma decomposição em primos.

Como n_1 tem comprimento $s = k + 1$, então

$$n_1 = p_1 p_2 \cdots p_k p_{k+1}, \text{ onde } p_1 \leq p_2 \leq \cdots \leq p_k \leq p_{k+1}$$

Suponha que haja mais uma decomposição em primos, de comprimento m. Então

$$n_1 = q_1 q_2 \cdots q_m, \text{ onde } q_1 \leq q_2 \leq \cdots \leq q_m$$

Assim, como q_m é o maior fator primo da segunda decomposição, tem-se que q_m é divisível por algum $p_i, 1 \leq i \leq k+1$; portanto, tem-se que

$$q_m \geq p_{k+1}. \tag{1.6}$$

Analogamente, p_{k+1} divide algum q_i e

$$p_{k+1} \geq q_m. \tag{1.7}$$

Assim, de (1.6) e de (1.7), temos que

$$p_{k+1} = q_m \tag{1.8}$$

.

Da igualdade

$$n_1 = p_1 p_2 \cdots p_k p_{k+1} = q_1 q_2 \cdots q_m$$

pode-se cancelar p_{k+1} e q_m devido a igualdade (1.8). Assim temos

$$p_1 p_2 \cdots p_k = q_1 \cdots q_{m-1}$$

Como estamos admitindo que todo n de comprimento k escreve-se de modo único como produto de primos, concluímos que cada p_i é igual a algum q_j e vice-versa. Assim, todo inteiro com $k + 1$ fatores primos admite apenas uma decomposição e o resultado segue por indução. □

O resultado do teorema é bastante importante para o estudo dos números primos, além de ser de extrema utilidade para o estudo da aritmética modular, que se baseia na divisão de inteiros por um determinado número.

Por fim, todo fundamento necessário para o estudo da aritmética modular está contido nessa seção.

Capítulo 2

Aritmética Modular

Este capítulo trata da Aritmética Modular, ramo da matemática que estuda a semelhança entre dois números inteiros que, ao serem divididos por um determinado número inteiro escolhido, tem o mesmo resto. No geral, este ramo estuda a repetição de restos de uma divisão entre inteiros.

2.1 Exemplos Prévios

2.1.1 Dias da Semana

Suponha que, em um mês, o primeiro dia do mês é domingo, o segundo é segunda-feira, e assim em diante, até chegarmos ao dia 8, que será novamente domingo. Observe que, a cada 7 dias, o dia da semana se repete. Assim, é possível descobrir em que dia da semana cairá o dia do mês apenas dividindo o número referente ao dia do mês e encontrando seu resto (que será chamado de r). Então:

- Se o r=1, o dia cairá num domingo. Por exemplo, o dia 15.
- Se r=2, é uma segunda-feira. Por exemplo, o dia 23.
- Se r=3, uma terça-feira.
- E assim em diante, até r=0, que cai aos sábados.

2.1.2 Meses de um ano

Também é possível identificar em que mês do ano a sociedade ocidental se encontra. Como um ano possui 12 meses, basta dividir a quantidade de meses que já passou por 12, de modo que o resto da divisão indica o mês que a sociedade se encontra (observação: restos de 1 a 11 indicam seus meses respectivos, resto igual a 0 indica o mês de dezembro), levando em consideração que a contagem se inicia a partir do início de um determinado ano. Por exemplo, se já passaram-se 23 meses do início de um determinado ano específico, significa que a pessoa está no mês de novembro, pois 23 dividido por 12 deixa resto igual a 11.

2.1.3 Restos de Inteiros

Ora, como percebe-se nos exemplos anteriores, a periodicidade se aplica ao próprio resto da divisão por algum inteiro qualquer. Por exemplo: na divisão por 5, os múltiplos de 5 deixam resto igual a 0, e os próximos quatro números sucessores a um múltiplo de 5 deixam restos iguais a 1, 2, 3 e 4, respectivamente.

De forma geral, para um inteiro n, os restos são:

$$0, 1, 2, ..., n-2, n-1$$

de modo que há n restos possíveis, variando de 0 a $n-1$. É esta repetição de restos da divisão por um inteiro que vai determinar a aritmética modular, pois dois inteiros que possuem o mesmo resto na divisão por um terceiro inteiro possuem características semelhantes, como será visto a seguir.

2.2 Congruência entre números inteiros: definições e propriedades iniciais

Como visto na seção 2.1.3, dois números inteiros podem possuir o mesmo resto na

divisão por um inteiro qualquer. Como exemplo prático, observa-se que os números 5 e 7 deixam resto 1 na divisão por 2, pois $5 = 2 \cdot 2 + 1$ e $7 = 2 \cdot 3 + 1$; observa-se também que os números 12 e 37 deixam resto igual a 2 na divisão por 5, pois $12 = 2 \cdot 5 + 2$ e $37 = 7 \cdot 5 + 2$. É possível generalizar essa "semelhança"entre dois inteiros, conforme a definição a seguir:

Definição 6. Sejam a, b e n números inteiros. Diz-se que dois números inteiros a e b são *congruentes módulo n*, o que é denotado por

$$a \equiv b \pmod{n},$$

quando ambos deixam o mesmo resto ao serem divididos por n.

Em linguagem matemática:

$$a \equiv b \pmod{n} \iff a = nk_1 + c \text{ e } b = nk_2 + c,\ k_1, k_2,\ c \in \mathbb{Z},\ 0 \leq c \leq n-1.$$

Se subtrairmos as igualdades $a = nk_1 + c$ e $b = nk_2 + c$, temos:

$$a - b = n(k_1 - k_2)$$

isto é, $a - b$ é um múltiplo de n.

Assim, a definição 6 pode ser reescrita da seguinte forma:

Definição 7. Sejam a, b e n três inteiros. Diz-se que *a é congruente a b módulo n* quando $a - b$ é um múltiplo de n.

Desta forma, sempre que houver dois inteiros com o mesmo resto na divisão por n, a subtração entre eles é um múltiplo de n. Por exemplo, 8-5 = 3 e três é um múltiplo de 3; assim, 8 é congruente a 5 módulo 3; note que tanto o 8 como o 5 deixam resto igual a 2 na divisão por 3.

Agora, observe os números 6, 51 e 101 e como se comportam na divisão por 5:

- Ora, 6 é congruente a si próprio.
- $6 - 51 = -45$ e -45 é um múltiplo de 5, de modo que $6 \equiv 51 \pmod{n}$. E tem-se que $51 - 6 = 45$, também um múltiplo de 5, de modo que $51 \equiv 6 \pmod{n}$.
- Já foi visto que 6 e 51 são congruentes módulo 5. Observe que $51 - 101 = -50$ e -50 é múltiplo de n, de modo que $51 \equiv 101 \pmod{5}$. Até aqui, tem-se que $6 \equiv 51 \equiv 101 \pmod{n}$. Veja que $6 - 101 = -95$ e 95 é múltiplo de n. Então $6 \equiv 101 \pmod{5}$.

Cada item acima pode ser generalizado em uma propriedade para cada um deles. Estas propriedades da congruência são: *reflexiva*, *simétrica* e *transitiva*.

Propriedade Reflexiva da Congruência. Todo número é congruente a si mesmo módulo n.

Demonstração. Pela hipótese, para $a \equiv a \pmod{n}$, é necessário mostrar que $a - a$ é múltiplo de n. Ora, $a - a = 0$ e 0 é múltiplo de qualquer inteiro n. □

Propriedade Simétrica. Se $a \equiv b \pmod{n}$ então $b \equiv a \pmod{n}$.

Demonstração. Ora, se $a \equiv b \pmod{n}$, então

$$a - b = nk,\ k \in \mathbb{Z}$$

Multiplicando a igualdade acima por -1, tem-se que

$$b - a = -kn$$

que equivale a $b \equiv a \pmod{n}$ □

Propriedade Transitiva. Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ então $a \equiv c \pmod{n}$.

Demonstração. Das hipóteses acima, tem-se que

$$a - b = k \cdot n \text{ e } b - c = l \cdot n$$

onde k e l são inteiros.
Ora, ao somar as duas equações acima, tem-se que

$$(a-b)+(b-c)=kn+ln$$
$$a-c=n(k+l)$$

de modo que $a-c$ é múltiplo de n, o que equivale a $a \equiv c \pmod{n}$. □

Note que a propriedade reflexiva é garantida por 0 ser divisível por n, o que corresponde a parte 1 da *Propriedade dos Múltiplos*. A propriedade transitiva é garantida por a soma de dois múltiplos de n ser também um múltiplo de n (vide demonstração), que corresponde a parte 2 da *Propriedade dos Múltiplos*. A propriedade simétrica implica em dizer que, se um número a é divisível por outro, seu múltiplo $-a$ também o será, o que corresponde a parte 3 da *Propriedade dos Múltiplos*.

2.3 Resíduos

Definição 8. Diz-se que um *sistema completo de resíduos módulo n* é um conjunto

$$\{a_0, a_1, a_2, ..., a_{n-1}\}$$

de inteiros tal que $a_0 \equiv 0 \pmod{n}$, $a_1 \equiv 1 \pmod{n}$ e assim em diante, até $a_{n-1} \equiv n-1 \pmod{n}$. Em particular, o conjunto de todos os restos de n é um sistema completo de resíduos módulo n.

Neste trabalho, o enfoque será dado ao sistema completo de resíduos formado pelos números inteiros não negativos menores que n, que são exatamente os possíveis restos da divisão de um inteiro positivo por n.

Seja a um inteiro positivo. Então, ao dividir por n, tem-se que

$$a = n \cdot k + r,\ 0 \leq r \leq n-1,$$

de modo que, subtraindo r dos dois lados da igualdade, tem-se que

$$a - r = nk,$$

isto é,

$$a \equiv r \pmod{n}$$

ou seja, todo inteiro positivo é congruente a seu resto módulo n e, neste caso, o resto será o resíduo de a módulo n. Ora, neste caso, o resíduo será *único*. De fato, sejam r e r' dois resíduos de um mesmo inteiro positivo módulo n, isto é

$$a \equiv r \pmod{n},\ 0 \leq r \leq n-1$$
$$a \equiv r' \pmod{n},\ 0 \leq r' \leq n-1$$

Então, usando a propriedade simétrica na primeira relação e a propriedade transitiva nas duas relações, tem-se que $r \equiv r' \pmod{n}$. Sem perda de generalidade, suponha $r \geq r'$. Como r e r' são congruentes módulo n, $r - r'$ é um múltiplo de n. Porém, pela condição estabelecida para os dois resíduos, conclui-se que $r - r' = 0$ e, por consequência, os resíduos são iguais.

A seguir, ilustramos a relação entre os restos de a e $-a$ na divisão por n. Suponha que a é negativo; então -a é positivo. Dividindo-o por n e fazendo as manipulações necessárias, com a condição $0 \leq r < n$ estabelecida para restos, tem-se que

$$-a = nq + r$$
$$a = n(-q) - r,$$

isto é,

$$a \equiv -r \pmod{n}, \tag{2.1}$$

de modo que, se r=0, nada temos que fazer. Se $r \neq 0$, tem-se que $(n - r) - (-r) = n$, que, em outras palavras, significa

$$-r \equiv n - r \pmod{n} \tag{2.2}$$

De (2.1) e (2.2), tem-se que $a \equiv n - r \pmod{n}$. Ora, como $r > 0$ e $r < n$, tem-se que $0 < n - r < n$, o que implica em $n - r$ ser o resto de a, sendo a negativo.

O que ilustramos acima é resumido na seguinte proposição.

Proposição 2.1. *Seja* $\{0, 1, 2, 3, ..., n-1\}$ *um sistema completo de resíduos. Sejam a e* $n > 1$ *inteiros e r o resto da divisão de* $|a|$ *por n. Então, o resíduo de a módulo n é igual a:*

- *0, se* $r = 0$*;*
- *r, se* $r \neq 0$ *e* $a \geq 0$*;*
- $n - r$*, se* $r \neq 0$ *e* $a < 0$*.*

Como exemplos da proposição acima, o número 55 tem resíduo 1 módulo 6, pois 55 é positivo e o resto da divisão de |55| por 6 é 1; já o número -55, por ser negativo e $|-55|$ deixar resto 1 na divisão por 6, tem resíduo igual a 6-1 = 5. Em outras palavras, 55 é congruente a 1 módulo 6 e -55 é congruente a 5 módulo 6.

Um exemplo mais interessante e complexo para o uso de resíduos está enunciado a seguir:

Exemplo 2.3.1. Se $p > 3$ é primo, então os resíduos de p módulo 6 são iguais a 1 ou a 5

Demonstração. Ora, 0 não é resíduo de p, pois se fosse, 6 dividiria p, que é primo. Temos que 1 é um resíduo possível, pois 7 deixa resto 1 na divisão por 6. Já o 2 não é um resíduo de p módulo 6, pois se fosse, $p \equiv 2 \pmod 6$ implica em $p - 2 = 6k$, isto é, $p - 2$ seria par, resultando em p par, o que não é possível pois p é primo maior que 3. Raciocínio análogo é usado para mostrar que 4 não é resíduo de p módulo 6. De imediato, 3 também não é resíduo de p módulo 6, pois se fosse, $p \equiv 3 \pmod 6$ implica em $p - 3 = 6k$, isto é, $p - 3$ seria múltiplo de 3, resultando em p também ser múltiplo de 3, o que não é possível pois p é primo maior que 3. Por fim, 5 é um resíduo possível, pois o próprio 5 é primo. □

O exemplo acima pode ser reescrito da seguinte forma: todo primo $p > 3$ é da forma 6k + 1 ou da forma 6k+5.

2.4 Somando e multiplicando congruências

Observe a seguinte situação: temos $1 \equiv 11 \pmod{10}$ e $2 \equiv 12 \pmod{10}$. Tem-se que $1 + 2 = 3$ é congruente a 3 módulo 10 e $11 + 12 = 23$ é também congruente a 3 módulo 10, pois tem resíduo igual a 3; assim, $3 \equiv 23 \pmod{10}$. Tem-se também que $1 \cdot 2 = 2$ é congruente a 2 módulo 10 e $11 \cdot 12 = 132$ é congruente a 2 módulo 10, pois tem resíduo igual a 2; assim, $2 \equiv 132 \pmod{10}$.

Observe que, no caso acima, ao somar as duas congruências módulo 10, obtém-se uma terceira congruência válida. O mesmo acontece ao multiplicar elas. O que aconteceu acima pode ser generalizado para toda e qualquer congruência entre inteiros.

Proposição 2.2. *Se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$*, então:*

- $a + b \equiv a' + b' \pmod{n}$*;*
- $a \cdot b \equiv a' \cdot b' \pmod{n}$

Demonstração. Ora, das hipóteses, tem-se que

$$a = a' + kn \tag{2.3}$$

e

$$b = b' + ln. \tag{2.4}$$

Somando (2.3) e (2.4), tem-se que

$$a + b = a' + b' + kn + ln$$
$$(a + b) - (a' + b') = n(k + l)$$

o que significa que

$$a + b \equiv a' + b' \pmod{n}.$$

Agora, multiplicando os lados das equações (2.3) e (2.4) e fazendo as manipulações algébricas

$$a \cdot b = (a' + kn)(b' + ln)$$
$$\Rightarrow a \cdot b = a' \cdot b' + a' \cdot ln + b' \cdot kn + kn \cdot ln$$
$$\Rightarrow a \cdot b = a' \cdot b' + n(a' \cdot l + b' \cdot k + k \cdot l \cdot n),$$

de modo que $a \cdot b - a' \cdot b'$ é um múltiplo de n, o que significa que

$$a \cdot b \equiv a' \cdot b' \pmod{n}.$$

□

Esta proposição será utilizada de forma indireta nas seções e capítulos a seguir.

Capítulo 3

Inversos módulo n

3.1 Aspectos iniciais

Lembre-se que o *inverso multiplicativo* de um número a, é o número a' que satisfaz $a \cdot a' = 1$. Por exemplo, o inverso multiplicativo de 5 é $\frac{1}{5}$, pois ao multiplicar um pelo outro, obtém-se o resultado igual a 1. A

Agora, trabalharemos com um conceito semelhante a este, mas dentro do contexto da aritmética modular. Começamos com um exemplo.

Exemplo 3.1.1. Observe a congruência módulo 7. A multiplicação entre 3 e 5 é igual a 15, que deixa resto 1 na divisão por 7. Então:

$$3 \cdot 5 \equiv 1 \pmod{7}$$

Exemplo 3.1.2. Agora, observe a congruência módulo 9. O resultado da multiplicação entre 5 e 2 deixa resto 1 na divisão por 9, de modo que

$$5 \cdot 2 \equiv 1 \pmod{9}$$

Estes exemplos nos levam a definir o conceito de inverso no contexto de congruências.

3.2 Inversos - definição, características e propriedades

Diz-se que um natural a e um número natural a' são *inversos módulo* n um do outro quando o produto entre eles é congruente a 1 módulo n, isto é: a é inverso módulo n de a' quando $a \cdot a' \equiv 1 \pmod{n}$. A primeira característica a se destacar é que, dentre os resíduos, o 0 não possui inverso módulo n pois

$$0 \cdot b \equiv 0 \pmod{n}, \text{ para todo } b \in \mathbb{Z}.$$

Além disso, 1 é seu próprio inverso módulo n, pois

$$1 \cdot 1 \equiv 1 \pmod{n}$$

Na seção anterior, foram vistos alguns exemplos da existência de inverso. Agora, é possível encontrar o inverso de 2 módulo 7, por exemplo:

- O número 1 é já descartado como inverso de 2 módulo 7, pois é seu próprio inverso;
- 2 não é seu próprio inverso, pois $2 \cdot 2 \equiv 4 \pmod{7}$;
- 3 não é inverso de 2 módulo n, pois $2 \cdot 3 \equiv 6 \pmod{n}$;
- Por fim, $2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$, de modo que 2 e 4 são inversos um do outro módulo n.

Usando raciocínio análogo ao usado acima, é possível encontrar os demais inversos módulo 7 de seus resíduos:

- 1 é seu próprio inverso.
- 2 é inverso de 4.
- 3 é inverso de 5.
- 4 é inverso de 2.

- 5 é inverso de 3.
- E, por fim, 6 é seu próprio inverso.

Observa-se que 6 é seu próprio inverso módulo 7, assim como 7 é seu próprio inverso módulo 8 e assim sucessivamente. É possível generalizar esta característica:

Proposição 3.1. *O inverso módulo n de $n-1$ é sempre ele mesmo.*

Demonstração. Ora,

$$(n-1)(n-1) = n^2 - 2n + 1 = n(n-2) + 1$$

o que equivale a dizer que

$$(n-1)(n-1) \equiv 1 \pmod{n}$$

isto é, n - 1 é seu próprio inverso módulo n. □

Ao analisar os resíduos módulo 7 e seus inversos, obtidos acima, nota-se que cada resíduo tem apenas um inverso módulo 7 (dentro do sistema completo de resíduos), de tal forma que este inverso é um dos restos de 7, excetuando o 0. Esta peculiaridade pode ser generalizada na seguinte propriedade:

Proposição 3.2. *Excluindo o 0, caso o resíduo módulo n admita inverso, este inverso é único dentre os restos.*

Demonstração. Suponha que a' e a'' sejam inversos de a módulo n, de forma que ambos sejam resíduos diferentes de 0. Assim:

$$a \cdot a' \equiv 1 \pmod{n} \tag{3.1}$$

e

$$a \cdot a'' \equiv 1 \pmod{n} \tag{3.2}$$

Multiplicando (3.1) por a'' tem-se que:

$$a'' \cdot (a \cdot a') \equiv a'' \cdot 1 \equiv a'' \pmod{n}$$

e multiplicando (3.2) por a' tem-se que

$$a' \cdot (a \cdot a'') \equiv a' \cdot 1 \equiv a' \pmod{n}$$

de modo que

$$a \cdot a' \cdot a'' \equiv a' \equiv a'' \pmod{n}$$

o que significa dizer que $a' - a''$ é múltiplo de n. Como ambos são resíduos, são positivos e menores que n, de modo que $-n < a' - a^{''} < n$. Como o único múltiplo de n entre -n e n é 0, então $a' - a'' = 0$, o que implica em a' e a'' serem iguais.

□

3.3 Quando o inverso modular existe?

Nesta seção, serão definidas as condições para a existência do inverso modular.

3.3.1 Exemplo Preliminar

Ao procurar o inverso de 2 módulo 8, nota-se que:

- $2 \cdot 2 = 4$;
- $2 \cdot 3 = 6$;
- $2 \cdot 4 = 8$;
- $2 \cdot 5 = 10$;
- $2 \cdot 6 = 12$;

de modo que 2 não tem inverso módulo 8. Note que 7 não pode ser inverso de 2, pois é inverso de si mesmo. Utilizando-se deste método, verifica-se que 3 (bem como 5 e 7) é inverso de si mesmo módulo 8, enquanto que os demais números não tem inverso. Ora, 3

e 8 são primos entre si, bem como 5 e 8, além de 7 e 8; os demais resíduos possuem, cada um, ao menos um fator primo em comum com o 8. Note também que:

- $2 \cdot 4 \equiv 0 \pmod 8$ e
- $6 \cdot 4 \equiv 0 \pmod 8$,

de modo que os resíduos são anulados módulo *8* por algum (ou alguns) outro resíduo que também não possui inverso e que também é um fator do número 8. Estas características podem ser generalizadas, como será feito a seguir:

Lema 1. *Se n e $1 < a < n$ são inteiros positivos com um fator primo $1 < p < n$ em comum, então a pode ser anulado módulo n pelo produto com um fator próprio de n.*

Demonstração. Estabelecidas as hipóteses, tem-se que

$$n = p \cdot c \quad \text{e} \quad a = p \cdot e,$$

onde c e e são cofatores de n e a, respectivamente. Da primeira equação e da condição estabelecida no enunciado do lema, tem-se que $1 < c < n$. Assim, nem a nem c são congruentes a 0 módulo n. Da primeira igualdade descrita acima, tem-se que

$$c \cdot p \equiv n \equiv 0 \pmod n \tag{3.3}$$

Ora,

$$c \cdot a \equiv c \cdot p \cdot e \pmod n \tag{3.4}$$

e, substituindo (3.3) em (3.4), tem-se que

$$c \cdot a \equiv n \cdot e \equiv 0 \cdot e \equiv 0 \pmod n$$

□

A última equação acima, bem como o cofator c de n, fará parte da demonstração do Teorema a seguir, importante para resultados futuros.

Teorema 3.3. *Se existir um fator primo comum entre a e n, então a não tem inverso módulo n.*

Demonstração. A demonstração é por contradição. Suponha que exista a' tal que $a \cdot a' \equiv 1 \pmod{n}$. Multiplicando esta igualdade pelo cofator c de n (usado no lema acima), tem-se que $c \cdot a \cdot a' \equiv c \pmod{n}$, mas, pela última igualdade da demonstração do lema acima, o produto entre c e a é congruente a 0 módulo n, de modo que

$$c \equiv c \cdot a \cdot a' \equiv 0 \cdot a' \equiv 0 \pmod{n},$$

de modo que n divide c, o que é impossível, pois $1 < c < n$. □

Este resultado é usado para determinar se um número inteiro possui ou não inverso módulo n. Por exemplo, se $n = 15$, os números 3, 5, 6, 9, 10 e 12 não possuem inverso módulo 15. Igualmente, os números 2, 3, 4, 6, 8 e 10 não possuem inverso módulo 12.

Há também um resultado, enunciado a seguir, necessário para o próximo Teorema:

Lema 2. *Se a e n não tem fatores próprios em comum, então a tem inverso módulo n.*

Demonstração. Ora,

$$a \cdot a' \equiv 1 \pmod{n} \iff a \cdot a' + n \cdot (-k) = 1 \tag{3.5}$$

para algum inteiro k de modo que, se a e n não admitem fator próprio comum, é necessário mostrar que existe inteiro k que satisfaça a equação acima.
Seja $V(a, n)$ o conjunto dos inteiros positivos da forma

$$x \cdot a + y \cdot n. \tag{3.6}$$

com x e y inteiros. Observe que esta equação é semelhante a equação (3.5). Se $1 \in V(a, n)$, 1 deverá ser seu menor elemento. Fazendo $x = 0$ e $y = 1$ em (3.6), nota-se que $n \in V(a, n)$. Suponha que m seja o menor dos números que pertence ao conjunto já destacado. Recorda-se que a e n são primos entre si. Ora,

$$m \in V(a, m),$$

isto é, existe x_1 e y_1 tais que

$$m = x_1 \cdot a + y_1 \cdot b.$$

Dividindo n por m e depois substituindo m e reorganizando a igualdade, tem-se que

$$\begin{aligned} n &= m \cdot q + r, \quad 0 \leq r < m \\ \Rightarrow n &= (x_1 \cdot a + y_1 \cdot b) \cdot q + r \\ \Rightarrow r &= (-x_1 \cdot q) \cdot a + (1 - y_1 \cdot q) \cdot n, \end{aligned}$$

o que implica em $r \in V(a, n)$, caso $r > 0$. Ora, como $r < m$, é impossível que r seja diferente de 0, pois, caso r fosse diferente de 0, $r \in V(a, n)$ entraria em contradição com o fato de m ser o menor elemento do conjunto. Portanto, $r = 0$ e, por consequência, m divide n.

De forma análoga ao procedimento acima, m divide a. Ora, se m divide n e a, $m = 1$, pois a e n são primos entre si. Assim, existe inteiro k que satisfaz a equação (3.5). □

Como consequência deste lema, se p for um primo, todos os resíduos de p possuem inverso módulo p.

Da combinação deste lema e do Teorema 3.3, tem-se o seguinte Teorema:

Teorema 3.4. *Sejam $a < n$ inteiros positivos. O resíduo a tem inverso módulo n se, e somente se, a e n não tem fatores primos em comum.*

A primeira implicação corresponde ao teorema 3.3, enquanto a recíproca corresponde ao lema 3. Uma consequência particular deste teorema, que trata sobre o cancelamento em congruências, será descrita a seguir:

Corolário 3.5. *Sejam $a < n$ números positivos sem fatores próprios comuns. Se*

$$a \cdot b \equiv a \cdot c \pmod{n},$$

para $a, b \in \mathbb{Z}$, então

$$b \equiv c \pmod{n}.$$

Demonstração. Se a e n não tem fatores próprios comuns então, pelo teorema 3.4, a tem inverso módulo n. Seja a' o inverso de a módulo n. Multiplicando os dois lados da igualdade presente na hipótese do corolário por a', tem-se que

$$a' \cdot a \cdot b \equiv a' \cdot a \cdot c \pmod{n}.$$

Como $a \cdot a' \equiv 1 \pmod{n}$, segue-se que $b \equiv c \pmod{n}$ □

A partir desse corolário, é possível afirmar que, da congruência $3 \cdot 10 \equiv 3 \cdot 15 \pmod{5}$, então 10 e 15 são congruentes módulo 5, pois 3 e 5 são primos entre si. Este corolário se torna mais útil quando o produto entre dois números se torna grande, de modo que o cancelamento simplificaria alguns cálculos.

3.3.2 Uma aplicação de Inverso

Proposição 3.6. *3 admite inverso 4k - 1 módulo 6k - 2, para k > 0.*

Demonstração. Para começar, é necessário demonstrar que 3 e 6k-2 são primos entre si. Como 3 é primo, $6k-2$ precisaria ser múltiplo de 3. Mas $6k-2 = 3(2k-1)+1$, de modo que este número não é divisível por 3.

Dito isso, pondo $n = 6k-2 = 3(2k-1)+1$:

$$\begin{aligned} 3(2k-1)+1 &\equiv 0 \pmod{n} \\ \Rightarrow 3(2k-1) &\equiv -1 \pmod{n} \\ \Rightarrow 3(1-2k) &\equiv 1 \pmod{n} \end{aligned}$$

onde 1-2k é o inverso de 3. Como k > 0, então 1-2k é negativo. Somando n a este número,

$$1 - 2k + 6k - 2 = 4k + 1.$$

Ora, 4k + 1 é, de imediato, maior que 0; além disto, como 1-2k é negativo e foi somado n a ele, 4k-1 é menor que n. Portanto 4k-1 é o inverso de 3 módulo 6k-2. □

Este resultado será importante no capítulo 4.

3.4 Inverso Módulo n e o Algoritmo Chinês do Resto

A característica da inversibilidade de m módulo n é utilizada para demonstrar um resultado importante dentro da aritmética modular, que é utilizado para solucionar um sistema de duas congruências (uma módulo m e outra módulo n) com uma mesma incógnita. O Teorema será enunciado a seguir:

Teorema 3.7 (Teorema Chinês do Resto)**.** *Sejam m e n inteiros positivos primos entre si. Se a e b são inteiros quaisquer, então o sistema*

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

sempre tem solução e qualquer uma de suas soluções pode ser escrita na forma

$$a + m \cdot (m' \cdot (b - a) + n \cdot t),$$

onde t é um inteiro qualquer e m' é o inverso de m módulo n.

Demonstração. Suponha que o inteiro x_0 seja a solução do sistema descrito no Teorema. Então

$$x_0 \equiv a \pmod{m} \tag{3.7}$$

$$x_0 \equiv b \pmod{n} \tag{3.8}$$

De (3.7) tem-se que

$$x_0 = a + m \cdot k,\ k \in \mathbb{Z} \tag{3.9}$$

Substituindo (3.9) em (3.8), tem-se que

$$a + m \cdot k \equiv b \pmod{n}$$

$$m \cdot k \equiv (b - a) \pmod{n} \tag{3.10}$$

Como m e n são primos, existe m' tal que $m \cdot m' \equiv 1 \pmod{n}$. Multiplicando m' dos dois lados da igualdade (3.10), tem-se que

$$k \equiv m' \cdot (b - a) \pmod{n}$$

$$\Rightarrow k = m'(b-a) + n \cdot t,\ t \in \mathbb{Z} \tag{3.11}$$

Substituindo (3.11) em (3.9), tem-se

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

Assim, se x_0 é solução do sistema de congruência, então x_0 é da forma $a+m(m'(b-a)+nt)$. Ora, note que

$$a + m(m'(b-a) + nt) \equiv a \pmod{n}$$

e que, considerando $mm' \equiv 1 \pmod{n}$

$$a + m(m'(b-a) + nt) \equiv a + m \cdot m'(b-a) \equiv a + 1(b-a) \equiv b \pmod{n}$$

mostrando que $x_0 = a+m(m'(b-a)+nt)$ é mesmo solução do sistema de congruências. □

Exemplo 3.4.1. Consideremos o seguinte problema:

"Determine o menor inteiro positivo que deixa resto 1 na divisão por 3 e resto 2 na divisão por 5."

Note que este problema pode ser reescrito em um sistema de congruências:

$$x \equiv 1 \pmod{3}$$
$$x \equiv 2 \pmod{5}$$

onde, usando o Teorema Chinês do Resto, $a = 1$, $b = 2$, $m = 3$ e $n = 5$. O inverso *m'* de 3 módulo 5 é 2. Assim, substituindo *a*, *b*, *m*, *n* e *m'* na expressão para a solução geral descrita no teorema, tem-se que

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

Fazendo $t = 0$, tem-se que o menor inteiro positivo é igual a 7.

3.4.1 Inversos e Potências Congruentes a 1 módulo *n*

Definição 9. Se n e $1 \leq b \leq n-1$ são inteiros, diz-se que a *ordem* de b módulo n é o menor inteiro positivo k para o qual $b^k \equiv 1 \pmod{n}$.

Note que, caso a ordem k exista, $b^{k+1} \equiv b^1 \pmod{n}$, $b^{k+2} \equiv b^2 \pmod{n}$ e assim sucessivamente, até que o expoente seja um múltiplo de k, de modo que $b^{mk} \equiv 1 \pmod{n}$, pois

$$b^{km} \equiv (b^k)^m \equiv 1^m \equiv 1 \pmod{n}$$

Como exemplo para a definição 9, considere as potências de 2 módulo 31. Observe que:

$$2^2 \equiv 4 \pmod{31};$$
$$2^3 \equiv 8 \pmod{31};$$
$$2^4 \equiv 16 \pmod{31};$$
$$2^5 \equiv 32 \equiv 1 \pmod{31}$$

de modo que a ordem de 2 módulo 31 é 5.

Considere, agora, as potências de 2 módulo 6:

$$2^1 \equiv 2 \pmod{6};$$
$$2^2 \equiv 4 \pmod{6};$$
$$2^3 \equiv 8 \equiv 2 \pmod{6};$$
$$2^4 \equiv 16 \equiv 4 \pmod{6}.$$

De forma geral, $2^{2k-1} \equiv 2 \pmod{6}$ e $2^{2k} \equiv 4 \pmod{6}$, para k inteiro positivo. Note que 2 e 6 são números pares. Generalizando esta ideia:

Proposição 3.8. *Se a e n são inteiros positivos pares, não existe inteiro positivo k tal que $a^k \equiv 1 \mod n$.*

Demonstração. Suponha que $a^k \equiv 1 \pmod{n}$. A congruência pode ser reescrita como

$$a^k - nt = 1,$$

o que é impossível pois, como n e a são pares, a subtração presente na igualdade acima também será. □

Uma outra propriedade, decorrente da Proposição 3.1, será descrita abaixo:

Proposição 3.9. *n-1 sempre tem ordem 2 módulo n.*

Agora, observe potências de 3 módulo 6 a seguir:

$$3^1 \equiv 3 \pmod 6;$$
$$3^2 \equiv 3 \pmod 6;$$
$$3^3 \equiv 3 \pmod 6.$$

Em geral, $3^k \equiv 3 \pmod n$. Note que o número 3, apesar de não ser par, também não possui ordem módulo 6. Note também que 3 e 6 não são primos entre si.

Há um resultado que indica a relação entre ordem e invertibilidade módulo n:

Proposição 3.10. *Se $1 \leq b \leq n-1$ tem ordem módulo $n \in \mathbb{N}$, então b e n são primos entre si.*

Demonstração. Da hipótese, tem-se que

$$b^k \equiv 1 \pmod n.$$

Para k=1, não há nada a mostrar. Para $2 \leq k$, tem-se que

$$b \cdot b^{k-1} \equiv 1 \pmod n,$$

implicando em b admitir inverso módulo n. Assim, pelo Teorema 3.4, b e n são primos entre si. □

Agora, observe estes casos particulares onde o módulo é primo:

$$2^4 \equiv 1 \pmod 5$$
$$3^4 \equiv 81 \equiv 1 \pmod 5$$
$$4^4 \equiv 256 \equiv 1 \pmod 5.$$

Note que 5 é primo, os números das bases das potências não tem fatores em comum com 5 e o expoente é o antecessor de 5. É possível generalizar esta característica para todos os números primos em um teorema descrito por Pierre de Fermat e demonstrado por Leonard Euler no século XVIII:

Teorema 3.11 (Pequeno Teorema de Fermat)**.** *Seja p um número primo e sejam a e p primos entre si. Então*

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

Demonstração. Para $a = 1$ não há nada a demonstrar. A demonstração abaixo serve para a diferente de 1. Ora, observe que os resíduos módulo p são

$$1, 2, 3, ..., p-1$$

que, ao serem multiplicados por a, obtem-se

$$1a, 2a, 3a, ..., (p-1)a.$$

Suponha que r_1 seja resíduo de a, r_2 resíduo de $2a$ e assim sucessivamente até r_{p-1} ser resíduo de $(p-1)a$. O produto destes resíduos pode ser calculados de duas formas.
Forma 1: Ora, $1a, 2a, 3a, ..., (p-1)a$ são congruentes aos seus respectivos resíduos $r_1, r_2, ..., r_{p-1}$ módulo p , de modo que, pela proposição 2.2, tem-se que

$$\begin{aligned} r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} &\equiv (1a)(2a)(3a) \cdots (p-1)a \pmod{p} \\ \Rightarrow r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} &\equiv a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdots (p-1)) \pmod{p} \end{aligned}$$

Forma 2: Considere os resíduos de p $r_1, r_2, ..., r_{p-1}$. Os resíduos são diferentes entre si, pois, se fossem iguais, supondo $r_k = r_l$, para k e l inteiros positivos menores que p, tem-se que

$$\begin{aligned} a \cdot k \equiv r_k \equiv r_l \equiv a \cdot l \pmod{p} \\ \Rightarrow a \cdot k \equiv a \cdot l \pmod{p}, \end{aligned}$$

onde é possível cancelar a, pois é possível usar o Corolário 3.5, já que a e p são primos entre si. Assim,

$$k \equiv l \pmod{p},$$

donde $k = l$, pois k e l são naturais menores que p. Assim, se $r_k = r_l$, então $k = l$. Portanto,

$$r_1, r_2, ..., r_{p-1}$$

são $p-1$ resíduos distintos entre si e não-nulos. Assim, por consequência, os resíduos sequenciados acima são equivalentes ao conjunto de resíduos possíveis de p, isto é,

$$1, 2, ..., p-1.$$

Assim:

$$r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} = 1 \cdot 2 \cdot 3 \cdots (p-1).$$

Combinando a última equação da forma 1 com esta última equação acima:

$$a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$$

O produto dos naturais menores que p acima é também um produto de inversíveis módulo p, sendo também inversível; logo, pelo Corolário 3.4, o produto dos naturais menores que p pode ser cancelado na equação anterior. Assim,

$$a^{p-1} \equiv 1 \mod p$$

□

Como consequência do Teorema de Fermat, tem-se o seguinte teorema:

Teorema 3.12. *Sejam p um primo, b um inteiro não divisível por p e k a ordem de b módulo p. A ordem k de b é um divisor de p-1.*

Demonstração. Ora, pelo Teorema de Fermat, $b^{p-1} \equiv 1 \pmod{p}$. Como k é ordem de b módulo p, então

$$k \leq p-1. \tag{3.12}$$

Dividindo $p-1$ por k, tem-se que

$$p-1 = kq + r, \tag{3.13}$$

onde q é um inteiro qualquer e r o resto da divisão feita, isto é, $1 \leq r \leq k-1$. Ora, como k é ordem, $b^k \equiv 1 \pmod{p}$, e então

$$1 \equiv b^{p-1} \equiv (b^k)^q \cdot b^r \pmod{p}, \tag{3.14}$$

donde $r = 0$, pois se r não fosse 0, r seria a ordem de b módulo p, o que contradiria a hipótese.
Substituindo $r = 0$ em (3.13), tem-se que $p - 1 = kq$, isto é, a ordem k de b é um divisor de $p - 1$. □

Estes dois teoremas serão bastante utilizados no capítulo seguinte, sendo que o primeiro de forma direta e o segundo de forma indireta.

Capítulo 4

A Criptografia RSA

A Criptografia RSA é uma criptografia de chave pública, isto é, de processo de codificação conhecido, criado em 1977 por três integrantes do Massachussets Institute of Technology (M.I.T), a saber, R.L. Rivest, A. Shamir e L. Adleman. A criptografia consiste em transformar uma mensagem (de texto, especificamente) em blocos de números com pelo menos dois algarismos que, por sua vez, serão transformados em outros números a partir da chave n, que é o produto entre dois primos distintos p e q. Estes dois primos devem ser mantidos em segredo entre o emissor e o receptor. Um terceiro indivíduo quebrará o código se, munido das ferramentas necessárias, fatorar o número n, o que é extremamente trabalhoso e duradouro se n for muito grande.

A seguir, será tratado sobre as fases de codificação e decodificação de uma mensagem dentro da Criptografia RSA, bem como os motivos que levam ao seu funcionamento.

4.1 Transformando uma mensagem em números

O primeiro passo para a codificação de uma mensagem dentro da Criptografia RSA é fazer a conversão de uma mensagem em números.

Suponha que a mensagem a ser enviada seja um texto. Cada letra do alfabeto repre-

sentará um número de dois dígitos, onde a letra "A"será substituída pelo número 10, a letra "B"pelo número 11 e assim sucessivamente, até a letra Z, que será substituída por 35. O espaço entre as palavras será substituído pelo número 99. Como exemplo, considere o nome "Joel Pereira dos Santos". Substituindo cada letra e cada espaço pelo número correspondente, tem-se que o nome será escrito como

$$19241421992514271418271099132428992810232924 28.$$

Em seguida, são escolhidos dois primos p e q, para gerar a chave pública $n = pq$. Neste caso, serão escolhidos primos da forma $6k+5$, a saber, $p = 17$ e $q = 23$, cujo produto n é igual a 391. Posteriormente, o número que representa o nome do autor será separado em blocos de números, de modo que cada bloco deverá ser um número menor que o produto n e não deve ser iniciado pelo algarismo 0. Neste caso, uma possível quebra em blocos do número acima é:

19-241-42-199-251-42-71-41-82-7-10-99-132-42-89-92-8-10-232-92-42-8

4.2 Codificação de uma mensagem

Antes de iniciar o processo de codificação a seguir, é necessário definir o produto entre os antecessores dos dois primos escolhidos (no caso usado na seção anterior, como p e q são da forma $6j+5$ e $6j_1+5$, então $(p-1)(q-1) = (6j+4)(6j_1+4) = 36j_1j+24j+24j_1+16$, de modo que este produto pode ser escrito na forma $6k-2$). Em seguida, tomando o produto obtido como módulo, devem ser escolhidos dois números c e d, usados, respectivamente, na codificação e na decodificação, que são inversos um do outro neste módulo (no caso que está sendo trabalhado, tomando d igual a $4k-1$, seu inverso módulo $6k-2$ é $c = 3$, como já foi visto na Proposição 3.6).

4.2.1 Como codificar a mensagem

Seja b um bloco pré-codificado e seja $\mathbf{C}(b)$ o bloco codificado. O bloco codificado será:

$$r \equiv b^3 \mod n$$

onde $r = \mathbf{C}(b)$ é o resto da divisão de b^3 por n, 3 é o valor de c apresentado anteriormente e n é o produto entre os primos p e q, já explicado na seção anterior. Assim, no exemplo do nome do autor, como $n = 391$, o bloco 19 pode ser codificado como 212, pois

$$212 \equiv 19^3 \pmod{391} \ .$$

Seguindo o mesmo raciocínio para os demais blocos, o conjunto de blocos da seção anterior pode ser codificado como

212-112-189-385-38-189-146-105-58-343-218-228-106-189-387-207-121-218-192-207-189-121

4.3 Decodificação

Para decodificar um bloco codificado denotado por a, é necessário ter posse da chave pública n e da chave privada d, além dos primos p e q que devem ser mantidos em segredo.

Seja $\mathbf{D}(a)$ o bloco decodificado de a. Então

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

Note que, como visto anteriormente

$$d = 4k - 1$$
$$(p-1)(q-1) = 6k - 2$$

Como $(p-1)(q-1) = 352$, tem-se que $352 = 6k - 2$ e, então, $k = 59$. Assim, $d = 235$. Calcular 212^{235} é impossível sem um computador, mas é possível usar o Teorema de Fermat e o Algoritmo Chinês do Resto para calcular a conta. A ideia é resolver 212^{235} módulo 17 e módulo 23, que são os fatores primos de 391. Ora,

$$212 \equiv 8 \pmod{17} \tag{4.1}$$

$$212 \equiv 5 \pmod{23} \tag{4.2}$$

Aplicando o Teorema de Fermat em (4.2), tem-se

$$5^{235} \equiv (5^{22})^{10}5^{15} \equiv 5^{15} \pmod{23}.$$

Como 23 é primo, a ordem de 5 módulo 23 é um dos divisores de $q-1 = 22$. Seus divisores são 1,2, 11 e 22, e é possível verificar que a ordem de 5 módulo 23 não é nem 1, nem 2 e nem 11, sendo, portanto, 22. Assim, é necessário dividir 5^{15} por 23, e, então

$$(5)^{15} \equiv 19 \pmod{23}$$

$$\Rightarrow 212^{235} \equiv 19 \pmod{23} \tag{4.3}$$

Aplicando o Teorema de Fermat em (4.1), tem-se

$$8^{235} \equiv (8^{16})^{14}8^{11} \equiv (2^3)^{11} \pmod{17}.$$

A ordem de 2 módulo 17 é 1, 2, 4, 8 ou 16, que são os divisores de 17-1 = 16. Portanto

$$(2^3)^{11} \equiv (2^3)^{11} \equiv (2^3)^8 \cdot (2^3)^3 \equiv 512 \equiv 2 \pmod{17}$$
$$\Rightarrow 8^{235} \equiv 2 \pmod{17}$$
$$\Rightarrow 212^{235} \equiv 2 \pmod{17}$$

Esta última congruência, juntamente com a congruência (4.3), formam o sistema

$$212^{235} \equiv 2 \pmod{17}$$
$$212^{235} \equiv 19 \pmod{23},$$

que pode ser reescrito na forma

$$x \equiv 2 \pmod{17}$$
$$x \equiv 19 \pmod{23}$$

Resolvendo este sistema da segunda congruência, tem-se que $x = 19 + 23y, y \in \mathbb{Z}$, que, substituindo na primeira congruência

$$19 + 23y \equiv 2 \pmod{17}$$
$$\Rightarrow 23y \equiv -17 \pmod{17}$$
$$\Rightarrow 23y \equiv 0 \pmod{17};$$

O 23 tem inverso 3 módulo 17, de modo que pode-se multiplicar a congruência acima por 3 e, então,

$$0 \cdot 3 \equiv 23y \cdot 3 \equiv y \equiv 0 \pmod{17}$$
$$\Rightarrow y \equiv 0 \pmod{17},$$

de modo que $y = 0$ é uma possível solução. Portanto,

$$x = 19 + 23y = 19 + 23 \cdot 0 = 19,$$

que é justamente o primeiro bloco b antes de sua codificação.

Todos os demais blocos se utilizam das mesmas ferramentas e do mesmo processo (em alguns casos, usando outras ferramentas de congruências já descritas aqui) para a decodificação.

4.4 Funcionamento da Criptografia RSA

Seja $n = pq$ a chave pública, onde p e q são primos mantidos em segredo. Sejam c e d, que são as chaves de codificação e decodificação, inteiros inversíveis entre si módulo $(p-1)(q-1)$ (justamente o produto usado para encontrar estas chaves), isto é, de tal forma que $c \cdot d \equiv 1 \pmod{(p-1)(q-1)}$, ou seja, $c \cdot d = 1 + k(p-1)(q-1)$. Considere b o bloco pré-codificado, $\mathbf{C}(b)$ o bloco codificado (onde $\mathbf{C}(b) \equiv b^c \pmod{n}$) e $\mathbf{D}(a)$ o bloco decodificado (onde $\mathbf{D}(a) \equiv a^d \pmod{n}$). Para garantir que a Criptografia RSA funcione, é necessário mostrar que, ao aplicar a decodificação a um bloco codificado a partir do bloco b, obtém-se de volta o bloco b. Em outras palavras, é necessário mostrar que

$$\mathbf{DC}(b) \equiv b \pmod{n}.$$

Substituindo $\mathbf{C}(b)$ e $\mathbf{D}(a)$ no lado esquerdo da congruência acima, pode-se concluir que é necessário mostrar que

$$b^{cd} \equiv b \pmod{n}.$$

Como $n = pq$ é necessário calcular os restos de b^{cd} módulo p e módulo q. Tomando, primeiramente, p, como $c \cdot d = 1 + (p-1)k(q-1)$, então

$$b^{cd} \equiv b^{1+(p-1)k(q-1)} \equiv b \cdot b^{(p-1)k(q-1)} \pmod{p}$$

e então

- Se p não divide b, então, pelo Teorema de Fermat, $b^{p-1} \equiv 1 \pmod{p}$ e, por consequência, $b^{cd} \equiv b \cdot 1^{k(q-1)} \equiv b \pmod{p}$;
- Se b divide p, tanto b como b^{cd} são congruentes a 0 módulo p e, então, $b^{cd} \equiv b \pmod{p}$;

Ou seja, para todo b inteiro positivo,

$$b^{cd} \equiv b \pmod{p}. \tag{4.4}$$

De forma inteiramente análoga,

$$b^{cd} \equiv b \pmod{q}. \tag{4.5}$$

As congruências (4.4) e (4.5) formam um sistema de congruências

$$\begin{aligned} b^{cd} &\equiv b \pmod{p} \\ b^{cd} &\equiv b \pmod{q}, \end{aligned}$$

onde b é uma solução de

$$\begin{aligned} x &\equiv b \pmod{p} \\ x &\equiv b \pmod{q}, \end{aligned}$$

que, pelo Teorema Chinês do Resto, tem solução geral

$$x = b + p(m'(b - b) + qt),$$

onde m' é o inverso de p módulo q. Note que $b - b = 0$ e o valor de x acima pode ser reescrito como

$$x = b + pqt,$$

cujos números b e b^{cd} são soluções. Assim,

$$b^{cd} = b + pqt \Rightarrow b^{cd} - b = pqt,$$

o que em termos de congruência de números inteiros, significa

$$b^{cd} \equiv b \pmod{pq}$$

como era necessário demonstrar.

Conclusão

A efetividade da Criptografia RSA é garantida devido ao tamanho dos números primos p e q, que são extremamente grandes, de modo que o produto $n = pq$ é um número maior ainda, o que torna extremamente inviável a fatoração.

Em geral, as chaves públicas usadas comercialmente pela Criptografia RSA usam, no mínimo, 200 algarismos. Mas existem chaves com mais de 2000 algarismos. Não existem métodos de fatoração conhecidos que sejam minimamente rápidos (minimante rápidos, aqui, se refere a quantidade de tempo em anos) para fatorar tal número n.

Além do mais, como consequência da chave n ser um número de muitos algarismos, o bloco pré-codificado b pode ser um bloco com muitos algarismos, de modo que, na codificação, o resíduo de b^c, que corresponde ao bloco codificado $\mathbf{C}(b)$, também pode ser grande, pois $1 \leq \mathbf{C}(b) \leq n$. No processo de decodificação, sem um computador é quase impossível calcular o resíduo de $\mathbf{C}(b)^d$ módulo n, pois além do bloco codificado poder ser grande, o número d também pode ser extremamente grande.

Um outro ponto a ser discutido é a existência dos números c e d. O número c só admite inverso se c e $(p-1)(q-1)$ forem primos entre si, isto é, possuírem 1 como único fator próprio comum. Este trabalho não tem como objetivo a obtenção geral de um inverso, mas é possível obter qualquer inverso d dado o número c a partir de uma extensão do Algoritmo de Euclides, onde $x \cdot c + (p-1)(q-1) \cdot 1 = MDC(c, (p-1)(q-1)) = 1$ e qualquer número $d \equiv x \mod (p-1)(q-1)$ é inverso de c módulo $(p-1)(q-1)$. Como exemplo, utilizando os valores de $(p-1)(q-1)$ e c usados no capítulo anterior como exemplo, tem-se que

$$3x + 352 = 1,$$

onde x = -117. Como é mais útil usar um valor de d positivo menor que $(p-1)(q-1)$, então, é necessário que

$$d = -117 + 352 = 235,$$

justamente o número usado no capítulo anterior.

Note novamente a importância de guardar secretamente os números p e q: conhecendo estes dois números, é possível encontrar o inverso d de c e, assim, decodificar facilmente a mensagem.

Referências Bibliográficas

[1] COUTINHO, S. C. **Criptografia**. IMPA, Rio de Janeiro, 2014.

[2] OSHIO, R. **Teorema Fundamental da Aritmética: o que ele diz?**. Estratégia Vestibulares. 2019. Disponível em: <https://vestibulares.estrategia.com/portal/materias/matematica/teorema-fundamental-da-aritmetica/> . Acesso em: 25 out. 2023.

[3] SANTOS, J. P. O. **Introdução a Teoria dos Números**. IMPA, Rio de Janeiro, 1998.