Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Criptografia RSA e a Teoria dos Números [†]

por

Roberval da Costa Lima

sob orientação do

Prof. Dr. Bruno Henrique Carvalho Ribeiro

Trabalho de conclusão apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática em Rede Nacional PROFMAT CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2013
João Pessoa - PB

[†]Este trabalho contou com apoio financeiro da CAPES.

L732c Lima, Roberval da Costa.

Criptografia RSA e a Teoria dos Números / Roberval da Costa Lima.– João Pessoa, 2013.

76f.

Orientador: Bruno Henrique Carvalho Ribeiro

Dissertação (Mestrado) - UFPB/CCEN

1. Matemática. 2. Criptografia RSA. 3. Teoria dos números. 4. Congruências. 5. Pequeno Teorema de Fermat.

UFPB/BC CDU: 51(043)

Criptografia RSA e a Teoria dos Números

por

Roberval da Costa Lima

Trabalho de conclusão apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática em Rede Nacional PROFMAT CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática

Aprovada por:

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

Prof. Dr. Antonio de Andrade e Silva - UFPB

Prof. Dr. Ricardo Rodrigues de Carvalho - URCA

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado Profissional em Matemática em Rede Nacional

13 de Agosto de 2013

Agradecimentos

Ao meu orientador Prof. Bruno Henrique C. Ribeiro pela paciência, pela compreensão e pela orientação deste trabalho.

Ao Prof. Antônio de Andrade e Silva pelo incentivo, insistente e sistemático. Infelizmente, não fui seu aluno, mas, tenho por ele uma grande admiração. Grande Prof. Andrade.

Aos meus professores de diversas épocas por mostrarem com maestria a beleza da matemática, cito aqui o nome de alguns: João Montenegro, Lenimar, Marivaldo, Abdoral (in memoriam), Marsicano (in memoriam), Chianca (in memoriam), Antonio Carlos (UFPE-1993), Jorge Hounie (UFPE-1993) e Roberto Bedregal (UFPE-1993).

A minha esposa Jucilene e minhas filhas Juciane e Jucielen pela compreensão e apoio na realização desse mestrado.

Aos colegas de curso, especialmente, Alysson Espedito, Diego e Aldeck pela ajuda nos grupos de estudo durante todo o mestrado.

Dedicatória

Aos meus pais, João Bento de Lima (in memoriam) e Irene da Costa Lima. Minha esposa Jucilene e minhas filhas Juciane e Jucielen.

Resumo

Neste trabalho apresentamos o conceito de criptografia, diferenciamos a criptografia simétrica da criptografia assimétrica e mostramos como funciona a criptografia RSA. Além disso, destacamos os principais resultados matemáticos que justificam o funcionamento desse criptossistema e sua segurança, tais como: congruências, Teorema de Euler, Pequeno Teorema de Fermat, Teorema de Wilson, Critério de Euler para resíduos quadráticos, Lei de Reciprocidade Quadrática e testes de primalidade.

Palavras chaves: Criptografia RSA, teoria dos números, congruências, Pequeno Teorema de Fermat.

Abstract

In this work we present the concept of cryptography, highlighting the differences between symmetric encryption and asymmetric encryption. We also show how RSA encryption works. Moreover, we study the main mathematical results that justify the operation of this cryptosystem and its security, such as: congruences, Euler's theorem, Fermat's Little Theorem, Wilson's Theorem, Euler's criterion for quadratic residues, Law of Quadratic Reciprocity and primality tests.

Keywords: RSA Encryption, number theory, congruence, Fermat's Little Theorem.

Sumário

Introdução

Este trabalho tem como objetivo principal explorar a matemática necessária para implementação do sistema criptográfico RSA. Além disso, deve servir como fonte inspiradora para estimular professores e alunos do ensino médio a ver que a matemática, mesmo tão abstrata, como é o caso dos resultados apresentados, principalmente nos capítulo 1 e 2, possui uma aplicação extremamente simples e inusitada como a criptografia RSA.

A criptografia é o estudo de métodos que permitam escrever mensagens em cifras ou códigos, de modo que apenas os legítimos destinatários sejam capazes de decodificar e ler as mensagens. Hoje em dia mais e mais pessoas e empresas utilizam a internet para se comunicar, tornando o uso da criptografia para manter o sigilo dessa comunicação cada vez mais importante. Por exemplo, bancos comerciais necessitam garantir que as transações entre seus clientes e o banco tenha a máxima segurança possível. No caso dos bancos essa segurança é ainda mais importante, pois, quase todas as suas transações passam pela internet e envolvem grandes valores monetários, mesmo aquelas realizadas nas agências bancárias. Nosso trabalho será baseado na criptografia RSA. Esse sistema criptográfico funciona da seguinte maneira: são criadas duas chaves, uma chave de codificação que será pública e uma chave de decodificação que será privada. Assim, se um usuário A deseja enviar uma mensagem para um usuário B, então A usa a chave de codificação de B para codificar a mensagem e envia essa mensagem codificada para B, quando B recebe a mensagem

codificada usa sua chave de decodificação, que apenas ele conhece, e decodifica a mensagem codificada, obtendo assim a mensagem original.

Ao longo dos três primeiros capítulos procuramos mostrar de forma sistemática e formal os principais resultados matemáticos que tornam possível a implementação do sistema criptográfico RSA. E, no último capítulo tentamos explorar esse criptossistema com um enfoque menos formal de modo que seja possível expor esse assunto para alunos do ensino médio.

Para desenvolver os conteúdos aqui estudados assumimos como conhecidos alguns tópicos elementares da teoria dos números, entre outros, citamos o princípio de indução, o algoritmo da divisão euclidiana e o máximo divisor comum. No entanto, no último capítulo abordamos informalmente o algoritmo da divisão euclidiana e o máximo divisor comum.

A implementação da criptografia RSA está totalmente baseada na aritmética das congruências. Daí, começamos nosso trabalho desenvolvendo os principais resultados sobre as congruências. Na seção 1 do primeiro capítulo descrevemos os aspectos aritméticos das congruências, mostrando como são feitas as manipulações com congruências e introduzindo o conceito de classe de equivalência, muito útil em algumas demonstrações, como foi o caso da demonstração do teorema de Euler e o teorema de Wilson. Na seção 2, introduzimos o conceito de equação modular e a função fi de Euler. Nesta seção apesar do título dá a entender que o objetivo principal seria o Teorema de Euler e o Teorema de Wilson, aqui demonstramos o Pequeno Teorema de Fermat que será usado para justificar o funcionamento do sistema RSA, apresentamos o conceito de ordem de um elemento do conjunto $\mathbb{Z}_n$, alguns resultados sobre essa ordem e a definição de raiz primitiva. Na seção 3, estudamos os resíduos quadráticos, introduzimos o Símbolo de Legendre, demonstramos o Critério de Euler e a Lei de Reciprocidade Quadrática, esses resultados não são necessários para a

implementação do sistema RSA, mas, são utilizados para demonstrar um dos testes de primalidade estudados no capítulo 2.

No capítulo 2 estudamos, na seção 1, como encontrar números primos com mais de 100 algarismos. Aqui apresentamos a função $\pi(x)$, o teorema dos números primos e fizemos uma estimativa do número de números primos com 100 algarismos que devemos testar para encontrar um número primo com 100 algarismos. Na seção 2 demonstramos alguns testes de primalidade e apresentamos, mas, não demonstramos o teste AKSL. Na verdade é nessa seção e na seção 3 do capítulo 1 que reside a matemática mais sofisticada. Essa matemática está intimamente ligada à segurança do sistema RSA, pois, para dificultar a fatoração de $n = pq$ necessitamos ter certeza que os números, p e q, escolhidos sejam realmente primos.

No capítulo 3 apresentamos, na seção 1, uma visão geral sobre o que é um sistema criptográfico diferenciando os criptossistemas simétricos e assimétricos. Nas seções 2 e 3 descrevemos, passo a passo, como funciona o sistema RSA e nas seções 4 e 5 abordamos alguns aspectos ligados a segurança do sistema RSA e o conceito de assinatura digital. E, por fim, na seção 6 fizemos dois exemplos para que o leitor veja como funciona esse sistema criptográfico.

O capítulo 4 apresenta a criptografia RSA com uma abordagem informal. Buscando através de exemplos mostrar toda a matemática necessária à implementação desse sistema, sem a preocupação de justificar porque esse sistema funciona e sem nos preocuparmos com a segurança. A abordagem dada aos conteúdos apresentados nesse capítulo tem como propósito facilitar a compreensão do sistema RSA para professores e alunos do ensino médio.

O presente trabalho teve as seções 1 e 2 do capítulo 1 baseadas em [3, 5] e a seção 3 foi influenciada por [6]. Já o capítulo 2 foi inspirado em [1, 4]. As seções 1 e 2 do capítulo 3 teve forte influência de [7, 8] e as demais seções foram baseadas

em [2]. O capítulo 4 é uma adaptação feita pelo autor desse trabalho do conteúdo apresentado no capítulo 3 para que seja possível aplicá-lo no ensino médio.

Capítulo 1

Congruências

Apresentaremos neste capítulo as congruências. Como o sistema criptográfico RSA usa essencialmente a aritmética dos restos então daremos a esse capítulo uma atenção maior, mostrando os principais resultados sobre as congruências. Além disso, as congruências estão relacionadas com todos os resultados usados, tanto para justificar porque o sistema RSA funciona quanto para demonstrar os testes de primalidade.

1.1 Aritmética dos Restos

Aqui mostraremos que a definição de congruência nos dará uma aritmética para os restos da divisão euclidiana por um dado número inteiro positivo. Veremos no capítulo 3 que essa aritmética é fundamental para a criptografia RSA.

Definição 1.1.1 *Dados a, b e n números inteiros, com $n > 1$. Dizemos que a e b são congruentes módulo n se na divisão euclidiana por n deixam o mesmo resto. E nesse caso escrevemos*

$$a \equiv b \mod n.$$

Na próxima proposição teremos um método para estabelecer se um dado número inteiro é ou não congruente a outro número inteiro. Alguns autores usam essa proposição como definição de congruência.

Proposição 1.1.1 *Seja $n \in \mathbb{Z}$, com $n > 1$. Sejam $a, b \in \mathbb{Z}$. Então*

$$a \equiv b \mod n \quad \Leftrightarrow \quad n|(a-b)$$

Demonstração: Se $a \equiv b \mod n$, então existem $q_1, q_2, r \in \mathbb{Z}$ tais que $a = q_1 n + r$ e $b = q_2 n + r$, com $0 \leq r < n$. Assim, $a - b = q_1 n - q_2 n = (q_1 - q_2)n$. Portanto, temos que $n|(a-b)$. Reciprocamente, suponha que $n|(a-b)$. Em seguida, divida a e b por n. Assim, existem $c_1, c_2, r_1, r_2 \in \mathbb{Z}$ tais que $a = c_1 n + r_1$, com $0 \leq r_1 < n$ e $b = c_2 n + r_2$, com $0 \leq r_2 < n$. Daí, resulta que $a - b = (c_1 - c_2)n + r_1 - r_2$, além disso, temos que $n|(a-b)$. Portanto, $a - b \equiv r_1 - r_2 \mod n$ e $a - b \equiv 0 \mod n$. Mas, pela definição de congruência temos que: como $a - b$ é congruente a $r_1 - r_2$, temos que esses números deixam o mesmo resto na divisão euclidiana por n, por outro lado, como $a - b$ é congruente a 0, temos que eles deixam o mesmo resto na divisão euclidiana por n, assim, temos que $r_1 - r_2$ e 0 deixam o mesmo resto na divisão euclidiana por n. Portanto, obtemos $r_1 - r_2 \equiv 0 \mod n$, mas, sabemos que $0 \leq r_1 < n$ e $0 \leq r_2 < n$, assim, obtemos $r_1 = r_2$. Logo, temos que $a \equiv b \mod n$ como queríamos demonstrar. ■

A proposição a seguir nos diz que a congruência é uma relação de equivalência sob o conjunto $\mathbb{Z}$. Além de ser de fundamental importância para podermos desenvolver os principais resultados das congruências ela é essencial para estabelecermos o conjunto das classes de equivalência e desenvolver a aritmética das classes de equivalência. Além disso, ela estabelece uma equivalência entre as congruências e as classes de equivalência, que será muito útil em muitas demonstrações como veremos adiante.

Proposição 1.1.2 *Seja $n \in \mathbb{Z}$, com $n > 1$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que:*

(1) $a \equiv a \mod n$,

(2) *Se* $a \equiv b \mod n$, *então* $b \equiv a \mod n$,

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

Demonstração:
(1) Como $n|0$, temos que $n|(a-a)$. Daí, obtemos que $a \equiv a \mod n$.
(2) Se $a \equiv b \mod n$, então $n|(a-b)$, isto é, existe um $q \in \mathbb{Z}$ tal que $a - b = qn$. Daí, temos que $b - a = (-q)n$, com $(-q) \in \mathbb{Z}$, assim, temos que $n|(b-a)$. Logo, $b \equiv a \mod n$.
(3) Se $a \equiv b \mod n$ e $b \equiv c \mod n$, então teremos que $n|(a-b)$ e $n|(b-c)$, o que implica $n|[(a-b)+(b-c)] = (a-c)$. Logo, temos que $a \equiv c \mod n$. ■

A proposição seguinte mostra que a relação de equivalência dada pela congruência é compatível com as operações de soma e produto em $\mathbb{Z}$. Esta compatibilidade é fundamental na manipulação aritmética dos restos.

Proposição 1.1.3 *Sejam $a, b, c, d, n \in \mathbb{Z}$, com $n > 1$. Se $a \equiv b \mod n$ e $c \equiv d \mod n$, então*

$$a + c \equiv b + d \mod n \qquad e \qquad ac \equiv bd \mod n.$$

Demonstração: Como $a \equiv b \mod n$ e $c \equiv d \mod n$, temos que $n|(a-b)$ e $n|(c-d)$, o que implica $n|(a-b)+(c-d) = (a+c)-(b+d)$. Daí, obtemos $a+c \equiv b+d \mod n$. Por outro lado, como $n|(a-b)$ e $n|(c-d)$, temos que existem q_1 e q_2 números inteiros tais que $a-b = q_1 n$ e $c-d = q_2 n$ o que implica $a = b+q_1 n$ e $c = d+q_2 n$. Daí, multiplicando membro a membro as duas igualdade obtemos $ac = bd + (bq_2 + dq_1 + q_1 q_2)n$, isto é, $ac - bd = (bq_2 + dq_1)n$ o que implica $n|(ac-bd)$. Portanto, temos que $ac \equiv bd \mod n$. ■

As duas proposições que se seguem mostram que vale a lei do cancelamento na adição e em certos casos específicos vale, também, a lei do cancelamento na multiplicação.

Proposição 1.1.4 *Sejam $a, b, c, n \in \mathbb{Z}$, com $n > 1$. Então*

$$a + c \equiv b + c \mod n \quad \Leftrightarrow \quad a \equiv b \mod n.$$

Demonstração: Como $a + c \equiv b + c \mod n$ temos, pela Proposição 1.1.1, que $n|[(a + c) - (b + c)] = (a - b)$. Portanto, pela Proposição 1.1.1 temos que $a \equiv b \mod n$. Reciprocamente, se $a \equiv b \mod n$, então pela Proposição 1.1.1 $n|(a - b) = [(a + c) - (b + c)]$. Logo, pela Proposição 1.1.1 temos que $a + c \equiv b + c \mod n$. ■

Proposição 1.1.5 *Sejam $a, b, c, n \in \mathbb{Z}$, com $n > 1$ e $mdc(c, n) = 1$. Então*

$$ac \equiv bc \mod n \quad \Leftrightarrow \quad a \equiv b \mod n.$$

Demonstração: Como $ac \equiv bc \mod n$, temos que $n|(ac - bc) = (a - b)c$. Como $mdc(c, n) = 1$ e $n|(a - b)c$, teremos que $n|(a - b)$. Sendo assim, obtemos $a \equiv b \mod n$. Reciprocamente, se $a \equiv b \mod n$, então $n|(a - b)$. Daí, temos que $n|(a - b)c = (ac - bc)$. Logo, temos que $ac \equiv bc \mod n$. ■

Proposição 1.1.6 *Sejam $a, b, c, n \in \mathbb{Z}$, com $n > 1$ e $mdc(c, n) = d$. Então*

$$ac \equiv bc \mod n \quad \Rightarrow \quad a \equiv b \mod \tfrac{n}{d}.$$

Demonstração: Se $ac \equiv bc \mod n$, então existe $k \in \mathbb{Z}$ tal que $ac - bc = (a - b)c = kn$. Daí, temos que $(a - b)\frac{c}{d} = k\frac{n}{d}$. Mas, $mdc(\frac{c}{d}, \frac{n}{d}) = 1$ (aqui usamos um resultado sobre mdc que não demonstramos. O leitor interessado poderá ver uma demonstração em [3]), o que implica $\frac{n}{d}$ divide $a - b$, isto é, $a \equiv b \mod \frac{n}{d}$ como queríamos demonstrar. ■

Definição 1.1.2 *Um sistema completo de resíduos módulo n é um conjunto S de n números que deixam todos os restos possíveis da divisão euclidiana desses números por n.*

Proposição 1.1.7 *Seja $S = \{r_1, r_2, \ldots, r_n\} \subseteq \mathbb{Z}$ um sistema completo de resíduos módulo n e sejam $a, b \in \mathbb{Z}$, com $mdc(a, n) = 1$, então*

$$S' = \{ar_1 + b, ar_2 + b, \ldots, ar_n + b\}$$

também é um sistema completo de resíduos módulo n.

Demonstração: Como $\{r_1, r_2, \ldots, r_n\}$ é um sistema completo de resíduos e $a, b \in \mathbb{Z}$, temos para cada $i = 1, 2, \ldots, n$, que $ar_i + b \equiv r_j \mod n$, para algum $j = 1, 2, \ldots, n$. Por outro lado, como os $r_i's$ formam um sistema completo de resíduos, se $i \neq j$, temos que $r_i \not\equiv r_j \mod n$. Como $mdc(a, n) = 1$ temos pela Proposição 1.1.5 que $ar_i \not\equiv ar_j \mod n$ e, daí, pela Proposição 1.1.4, temos que $ar_i + b \not\equiv ar_j + b \mod n$. Portanto, provamos que os elementos do conjunto S' são dois a dois incongruentes e como S' possui n elementos que são congruentes aos elementos de S, concluímos que $\{ar_1 + b, ar_2 + b, \ldots, ar_n + b\}$ é um sistema completo de resíduos.

■

Como dado $a \in \mathbb{Z}$, pelo algoritmo da divisão euclidiana, temos que existem $q, r \in \mathbb{Z}$ tais que $a = qn + r$, com $0 \leq r < n$, então a Proposição anterior nos garante que qualquer sistema completo de resíduos módulo n tem seus elementos congruentes aos elementos do conjunto $\{0, 1, 2, \ldots, n-1\}$, em alguma ordem.

A próxima definição servirá para estabelecermos uma nova forma de lidarmos com as congruências, em alguns casos simplificando os cálculos em algumas demonstrações.

Definição 1.1.3 *Dado $a \equiv b \mod n$, temos que $\exists k \in \mathbb{Z}$ tal que $a - b = kn$. Chamamos de classe de equivalência de a em relação a congruência módulo n o conjunto $\overline{a} = \{a + kn : k \in \mathbb{Z}\}$.*

A próxima proposição nos mostra como relacionar as congruências com as classes de equivalência. Ela nos permite passar de uma forma de notação para outra. Isto é, mostra a relação de equivalênca entre as duas formas de tratar com os restos da divisão euclidiana por um dado número.

Proposição 1.1.8 *Sejam $a, b, n \in \mathbb{Z}$, $n > 1$. Então, $a \equiv b \mod n$ se, e somente se, $\overline{a} = \overline{b}$.*

Demonstração: Se $x \in \overline{a}$, então existe $k \in \mathbb{Z}$ tal que $x = a+kn$, isto é, $x-a = kn$, o que implica $x \equiv a \mod n$. Como $a \equiv b \mod n$, pela Proposição 1.1.2 item (3), temos que $x \equiv b \mod n$. Portanto, existe $k' \in \mathbb{Z}$ tal que $x - b = k'n$. Logo, $x \in \overline{b}$. Por outro lado, se $x \in \overline{b}$, então existe um $c \in \mathbb{Z}$ tal que $x = b+cn$, isto é, $x-b = cn$. Portanto, $x \equiv b \mod n$. Como $a \equiv b \mod n$, novamente pela Proposição 1.1.2 item (2) e (3), temos que $x \equiv a \mod n$. Daí, temos que existe $c' \in \mathbb{Z}$ tal que $x-a = c'n$, isto é, $x = a + c'n$. Logo, $x \in \overline{a}$. Portanto, temos que $\overline{a} = \overline{b}$. Reciprocamente, se $\overline{a} = \overline{b}$, então $a + 0n = a \in \overline{b}$, isto é, existe $k \in \mathbb{Z}$ tal que $a = b + kn$. Daí, temos que $a - b = kn$, isto é, $a \equiv b \mod n$. ■

Definição 1.1.4 *O conjunto de todas as classes de equivalência é chamado de conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo n. E será denotado por $\mathbb{Z}_n$.*

Proposição 1.1.9 *Se $n \in \mathbb{Z}$ e $n > 1$, então $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ é um conjunto contendo exatamente n classes de equivalências.*

Demonstração: Sejam $a, b \in \mathbb{Z}$ tais que $0 \leq a < b < n$. Então $b - a \neq 0$ e $n \nmid (b - a)$. Portanto, teremos que $a \not\equiv b \mod n$. Logo, pela Proposição anterior temos que $\overline{a} \neq \overline{b}$. Assim, $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\} \subseteq \mathbb{Z}_n$ é um conjunto com exatamente n elementos. Para provar a igualdade é suficiente mostrar que: dado $a \in \mathbb{Z}$ então $\overline{a} \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$. Pelo algoritmo da divisão temos que, $\exists q, r \in \mathbb{Z}$ tais que $a = qn + r$, com $0 \leq r < n$. Daí, teremos que $a \equiv r \mod n$, com $0 \leq r < n$, isto é, $\overline{a} = \overline{r} \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ como queríamos mostrar. ■

Proposição 1.1.10 *Seja $n \in \mathbb{Z}$. Se $\overline{a} = \overline{b}$ e $\overline{c} = \overline{d}$, então*

(1) $\overline{a + c} = \overline{b + d}$

(2) $\overline{ac} = \overline{bd}$

Demonstração: Segue imediato da Proposição 1.1.3 e da Proposição 1.1.8. ■

Definição 1.1.5 *Seja n um número inteiro, $n > 1$. Definimos a soma e o produto de duas classes de equivalência por*

(1) $\overline{a} + \overline{b} = \overline{a + b}$

(2) $\overline{a} \cdot \overline{b} = \overline{ab}$

Observe que a Proposição 1.1.10 nos garante que estas operações estão definidas.

Definição 1.1.6 *Dado $\overline{a} \in \mathbb{Z}_n$. Dizemos que $\overline{b}$ é o inverso multiplicativo de $\overline{a}$ quando $\overline{a} \cdot \overline{b} = \overline{1}$.*

Essa definição é muito importante, pois, como veremos adiante o conjunto de todos os elementos que possuem inverso em $\mathbb{Z}_n$ é fechado com relação a multiplicação.

Proposição 1.1.11 *A classe $\overline{a}$ tem inverso multiplicativo em $\mathbb{Z}_n$ se, e somente se, a e n são coprimos.*

Demonstração: Se $\overline{a}$ tem inverso multiplicativo em $\mathbb{Z}_n$, então existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$, isto é, $\overline{ab} = \overline{1}$. Portanto, temos que $ab \equiv 1 \mod n$. Daí, temos que $n|(ab-1)$, isto é, existe $q \in \mathbb{Z}$ tal que $ab - 1 = qn$. Assim, obtemos que existem $b, q \in \mathbb{Z}$ tais que $ba - qn = 1$. Logo, temos que a e n são coprimos. Reciprocamente, se a e n são coprimos, então existem $x, y \in \mathbb{Z}$ tais que $xa + yn = 1$. Assim, temos que $n|(xa-1)$, isto é, $xa \equiv 1 \mod n$. Portanto, temos que $\overline{xa} = \overline{x} \cdot \overline{a} = \overline{1}$, ou seja, existe um $\overline{x} \in \mathbb{Z}_n$ que é o inverso multiplicativo de $\overline{a}$. ■

Definição 1.1.7 *Os elementos invertíveis de $\mathbb{Z}_n$ formam um conjunto que chamamos de conjunto reduzido de resíduos módulo n. E será denotado por $\mathbb{Z}_n^*$.*

Proposição 1.1.12 *Se $\overline{a}, \overline{b} \in \mathbb{Z}_n^*$, então $\overline{ab} \in \mathbb{Z}_n^*$.*

Demonstração: Como $\overline{a}, \overline{b} \in \mathbb{Z}_n^*$ temos que $\exists \overline{x}, \overline{y} \in \mathbb{Z}_n^*$ tais que $\overline{a} \cdot \overline{x} = \overline{1}$ e $\overline{b} \cdot \overline{y} = \overline{1}$. Portanto, teremos que $\overline{ab} \cdot \overline{xy} = \overline{abxy} = \overline{axby} = \overline{a} \cdot \overline{x} \cdot \overline{b} \cdot \overline{y} = \overline{1} \cdot \overline{1} = \overline{1}$. Portanto temos que $\overline{ab} \in \mathbb{Z}_n^*$. ■

Na Proposição anterior provamos que o conjunto $\mathbb{Z}_n^*$ é fechado com relação ao produto.

Proposição 1.1.13 *Seja $\overline{b} \in \mathbb{Z}_n^*$. Então, $\forall a \in \mathbb{Z}$ tal que $mdc(a, n) = 1$ tem-se que $\overline{ab} \in \mathbb{Z}_n^*$.*

Demonstração: Como $\overline{b} \in \mathbb{Z}_n^*$ temos pela Proposição 1.1.11, que $mdc(b, n) = 1$, daí, temos que existem $x_1, y_1 \in \mathbb{Z}$ tais que $bx_1 + ny_1 = 1$. Mas, $mdc(a, n) = 1$, daí, existem $x_2, y_2 \in \mathbb{Z}$ tais que $ax_2 + ny_2 = 1$. Assim, multiplicando membro a membro as duas últimas igualdades obtemos $x_1x_2(ab) + (x_2y_1a + x_1y_2b + y_1y_2n)n = 1$, o que

implica $mdc(ab, n) = 1$. Portanto, novamente pela Proposição 1.1.11, temos que $\overline{ab} \in \mathbb{Z}_n^*$ como queríamos demonstrar. ■

Nesta seção descrevemos os principais resultados sobre as congruências e fizemos uma relação entre as congruências e as classes de equivalência. Estes resultados serão fundamentais para provarmos os resultados apresentados nas duas próximas seções.

1.2 Os Teoremas de Euler e Wilson

Nesta seção introduzimos o conceito de equação modular e a função fi de Euler. Além disso, demonstramos o teorema de Euler, o teorema de Wilson e o pequeno teorema de Fermat que será usado para justificar o funcionamento do sistema RSA. Também estudamos um pouco sobre raiz primitiva e sobre a ordem de um elemento do conjunto $\mathbb{Z}_n$.

Proposição 1.2.1 *Sejam $a, n \in \mathbb{Z}$, com $n > 1$, então a congruência $aX \equiv 1 \mod n$ possui uma solução x_0 se, e somente se, a e n são coprimos. Além disso, x é outra solução da congruência se, e somente se, $x \equiv x_0 \mod n$.*

Demonstração: Suponha que x_0 seja solução da congruência acima. Isto é, $ax_0 \equiv 1 \mod n$. Assim, $n|(ax_0 - 1)$, isto é, $\exists y \in \mathbb{Z}$ tal que $ax_0 - 1 = yn$. Assim, teremos que $x_0a - yn = 1$. Portanto, temos que a e n são coprimos. Reciprocamente, se a e n são coprimos, então existem $x_0, y \in \mathbb{Z}$ tais que $x_0a + yn = 1$, assim, podemos escrever $ax_0 - 1 = (-y)n$, onde $(-y) \in \mathbb{Z}$. Daí, temos que $ax_0 \equiv 1 \mod n$. Logo, x_0 é solução da congruência $aX \equiv 1 \mod n$.

Além disso, se x é outra solução da congruência $aX \equiv 1 \mod n$, então $ax \equiv 1 \mod n$. Por outro lado, x_0, também é solução, isto é, $ax_0 \equiv 1 \mod n$. Sendo assim,

temos que $ax \equiv ax_0 \mod n$. Como $mdc(a,n) = 1$ temos pela Proposição 1.1.5, que podemos cancelar o a e obter $x \equiv x_0 \mod n$, como queríamos demonstrar. ■

Definição 1.2.1 *Seja n um número natural com $n > 1$. Chamamos de função fi de Euler, denotada por $\phi(n)$, a função definida pelo número de elementos invertíveis em $\mathbb{Z}_n$.*

Observe que $\phi(n) \leq n-1$. Além disso, temos que $\phi(n) = n-1$ se, e somente se, n é um número primo.

Mais adiante mostraremos como calcular $\phi(n)$ em geral. Iremos agora verificar algumas propriedade da função fi de Euler.

Teorema 1.2.1 *Sejam $m, n \in \mathbb{N}$, com $mdc(m,n) = 1$. Então*

$$\phi(mn) = \phi(m)\phi(n).$$

Demonstração: Vamos dispor os números de 1 até mn da seguinte forma:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m & 2m & 3m & \cdots & nm \end{array}$$

Se na linha r, onde estão os termos $r, m+r, 2m+r, ..., (n-1)m+r$, tivermos $mdc(m,r) = d > 1$, então nenhum termo dessa linha será primo com mn, uma vez que estes termos, sendo da forma $km+r$, com $0 \leq k \leq n-1$, são todos divisíveis por d. Logo, para encontrarmos os naturais desta tabela que são primos com mn, devemos olhar na linha r somente se $mdc(m,r) = 1$. Portanto, temos $\phi(m)$ linhas em que todos os elementos são primos com m.

Agora devemos procurar em cada uma dessas $\phi(m)$ linhas, quantos elementos são primos com n, uma vez que todos são primos com m. Como $mdc(m,n)=1$ os elementos $r, m+r, 2m+r, ..., (n-1)m+r$ formam um sistema completo de resíduos módulo n. Logo, cada uma destas linhas possui $\phi(n)$ elementos primos com n e, portanto, como eles são primos com m, eles são primos com mn. Isto nos garante que $\phi(mn)=\phi(m)\phi(n)$. ■

Lema 1.2.1 *Se p é um número primo e $r \in \mathbb{N}$, então temos*

$$\phi(p^r) = p^r - p^{r-1} = p^r(1-\tfrac{1}{p}).$$

Demonstração: De 1 até p^r, temos p^r números naturais. Temos que excluir desses os números que não são primos com p^r, ou seja, todos os múltiplos de p, que são $p, 2p, ..., p^{r-1}p$, cujo número é p^{r-1}. Portanto, $\phi(p^r) = p^r - p^{r-1}$. ■

Teorema 1.2.2 *Para $n = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_r^{\alpha_r}$, com p_i primo e $\alpha_i \in \mathbb{N}$, $i = 1, \ldots, r$, temos*

$$\phi(n) = n(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})\cdots(1-\tfrac{1}{p_r}).$$

Demonstração: O Teorema 1.2.1 nos garante que $\phi(n) = \phi(p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_r^{\alpha_r}) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\cdots\phi(p_r^{\alpha_r})$. Por outro lado, o Lema 1.2.1, permite escrever este último resultado assim: $\phi(n) = p_1^{\alpha_1}(1-\frac{1}{p_1})p_2^{\alpha_2}(1-\frac{1}{p_2})\cdots p_r^{\alpha_r}(1-\frac{1}{p_r}) = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$. Portanto, teremos que $\phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$ como queríamos demonstrar. ■

Teorema 1.2.3 (Euler) *Sejam $n, a \in \mathbb{Z}$, com $mdc(a,n)=1$. Então,*

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

Demonstração: Seja $\mathbb{Z}_n^* = \{\overline{r_1}, \overline{r_2}, \ldots, \overline{r_{\phi(n)}}\}$ o conjunto dos elementos invertíveis de $\mathbb{Z}_n$. Além disso, temos que $\overline{a^{\phi(n)}} \cdot \overline{r_1} \cdot \overline{r_2} \cdots \overline{r_{\phi(n)}} = \overline{ar_1} \cdot \overline{ar_2} \cdots \overline{ar_{\phi(n)}}$. Como $mdc(a,n) = 1$ temos pela Proposição 1.1.13, que $\overline{ar_i} \in \mathbb{Z}_n^*$, para cada $i \in \{1, 2, \ldots, \phi(n)\}$. Por outro lado, se $i \neq j$, tem-se que $\overline{r_i} \neq \overline{r_j}$, o que implica $\overline{ar_i} \neq \overline{ar_j}$, pois, $mdc(a,n) = 1$. Assim, teremos que $\overline{ar_1} \cdot \overline{ar_2} \cdots \overline{ar_{\phi(n)}} = \overline{r_1} \cdot \overline{r_2} \cdots \overline{r_{\phi(n)}}$. Portanto, $\overline{a^{\phi(n)}} \cdot \overline{r_1} \cdot \overline{r_2} \cdots \overline{r_{\phi(n)}} = \overline{r_1} \cdot \overline{r_2} \cdots \overline{r_{\phi(n)}}$. Logo, multiplicando cada membro da última igualdade pelo respectivo inverso dos $r_i's$, obtemos $\overline{a^{\phi(n)}} = \overline{1}$, isto é, $a^{\phi(n)} \equiv 1 \mod n$ como queríamos demonstrar. ■

Corolário 1.2.1 (Pequeno Teorema de Fermat) *Sejam $a, p \in \mathbb{Z}$, com p primo e $mdc(a,p) = 1$. Então*

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

Demonstração: Como $\phi(p) = p - 1$ e $mdc(a,p) = 1$, o resultado segue direto do Teorema 1.2.3. ■

Proposição 1.2.2 *Sejam $a, n \in \mathbb{Z}$, com $a > 1$ e $n > 1$. Então*

$$\exists r \in \mathbb{Z}, r > 0, \text{ tal que } a^r \equiv 1 \mod n \quad \Leftrightarrow \quad mdc(a,n) = 1$$

Demonstração: Se $mdc(a,n) = 1$, então o Teorema de Euler nos garante que existe $\phi(n) = r \in \mathbb{Z}$ tal que $a^r \equiv 1 \mod n$. Reciprocamente, suponha que $mdc(a,n) > 1$. Então a equação $aX - nY = 1$ não possui solução e, daí, a equação modular $aX \equiv 1 \mod n$ não possui solução. Consequentemente, não pode existir $r \in \mathbb{Z}$, $r > 0$ tal que $a^r \equiv 1 \mod n$. Logo, concluímos que $mdc(a,n) = 1$. ■

O próximo lema servirá para provarmos o teorema de Wilson.

Lema 1.2.2 *Seja $a \in \mathbb{Z}$, com $a > 4$ um número composto, então $a|(a-1)!$.*

Demonstração: Seja $a \in \mathbb{Z}$ um número composto e $a > 4$. Então existem $a_1, a_2 \in \mathbb{Z}$ tais que $a = a_1 a_2$, com $1 < a_1 \leq a_2 < a$. Sendo assim, teremos que $(a-1)! = 1 \cdots a_1 \cdots a_2 \cdots (a-1)$. Portanto, temos que $a|(a-1)!$ como queríamos demonstrar. ■

Teorema 1.2.4 (Wilson) *Seja $p \in \mathbb{Z}$, $p > 1$. Então*

$$p \text{ é um número primo} \quad \Leftrightarrow \quad (p-1)! \equiv p-1 \mod p.$$

Demonstração: Se p é um número primo então $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ são os elementos invertíveis de $\mathbb{Z}_p$. Além disso, se $x \in \mathbb{Z}_p$ é tal que $\overline{x}^2 = \overline{1}$, então $x^2 \equiv 1 \mod p$, isto é, $p|(x^2-1) = (x-1)(x+1)$. Daí, temos $p|(x-1)$ ou $p|(x+1)$. Mas, $0 \leq x < p$ e p é primo. Assim, teremos que $x = 1$ ou $x = p-1$. Logo, todos os elementos de $\mathbb{Z}_p^*$, com excessão de $\overline{1}$ e $\overline{p-1}$, possuem inverso diferente dele próprio. Portanto, temos que: $\overline{2} \cdots \overline{(p-2)} = \overline{1}$. Assim, obtemos $2 \cdots (p-2) \equiv 1 \mod p$. Logo, temos que $(p-1)! = 1 \cdot 2 \cdots (p-2)(p-1) \equiv p-1 \mod p$. Reciprocamente, suponha que $(p-1)! \equiv p-1 \mod p$ e que $p > 4$ não é primo. Então pelo Lema 1.2.2 podemos garantir que $p|(p-1)!$. Como $p > 4$ $p \nmid (p-1)$. Sendo assim, temos que $p \nmid [(p-1)! - (p-1)]$. Logo, $(p-1)! \not\equiv p-1 \mod p$ o que contradiz nossa hipótese. Agora observe que $3! = 6 \not\equiv 3 \mod 4, 2! = 2 \equiv 2 \mod 3$ e $1! \equiv 1 \mod 2$. Portanto, se $(p-1)! \equiv p-1 \mod p$ então p é um número primo. ■

Observe que o Teorema de Wilson caracteriza todos os números primos, isto é, todo número que obedece o teorema é um número primo e, reciprocamente, todo número primo obedece esse teorema.

Os resultados apresentados até o final dessa seção serão utilizados para provarmos alguns testes de primalidade apresentados no capítulo 2. A seguir descreveremos alguns resultados sobre a ordem de um elemento de $\mathbb{Z}_n$ e sobre a raiz primitiva módulo n.

Pelo Teorema de Euler temos que se $a, n \in \mathbb{Z}$, com $mdc(a,n) = 1$ e $n > 1$, então $a^{\phi(n)} \equiv 1 \mod n$. Portanto, existe um menor expoente k tal que $a^k \equiv 1 \mod n$. Este menor valor de k poderá ser menor do que $\phi(n)$. Por exemplo, $mdc(3,8) = 1$, assim, pelo Teorema de Euler, temos que $3^{\phi(8)} \equiv 1 \mod 8$, mas, $3^2 \equiv 1 \mod 8$ e $2 < 4 = \phi(8)$.

Definição 1.2.2 *O menor inteiro positivo k para o qual $a^k \equiv 1 \mod n$, onde $mdc(a,n) = 1$, é chamado de ordem de a módulo n e denotado por $ord_n a$.*

Proposição 1.2.3 *Seja $k = ord_n a$. Então*

$$a^h \equiv 1 \mod n \Leftrightarrow k|h.$$

Demonstração: Dados $h, k \in \mathbb{Z}$, com $k \neq 0$, então pelo algoritmo da divisão temos que existem $q, r \in \mathbb{Z}$ tais que $h = qk + r$, com $0 \leq r < k$. Sendo assim, temos que $a^h = a^{qk+r} = (a^k)^q a^r$. Por outro lado, $k = ord_n a$, isto é, $a^k \equiv 1 \mod n$. Portanto, concluímos que $a^h = a^{qk+r} = (a^k)^q a^r \equiv 1^q a^r \equiv a^r \mod n$. Além disso, $a^h \equiv 1 \mod n$, por hipótese. Logo, temos $a^r \equiv 1 \mod n$. Mas, como $0 \leq r < k$ e k por definição é o menor inteiro positivo tal que $a^k \equiv 1 \mod n$, temos que $r = 0$. Portanto, $h = qk$, isto é, $k|h$. Reciprocamente, se $k \mid h$, então existe $q \in \mathbb{Z}$ tal que $h = qk$, daí, $a^h = a^{qk} = (a^k)^q \equiv 1^q = 1 \mod n$. ■

Corolário 1.2.2 *$ord_n a|\phi(n)$.*

Demonstração: Pelo Teorema de Euler, temos que $a^{\phi(n)} \equiv 1 \mod n$, se $mdc(a,n) = 1$. Daí, o Teorema que acabamos de demonstrar nos garante que $ord_n a|\phi(n)$. ■

Proposição 1.2.4 *Seja $k = ord_n a$. Então $a^t \equiv a^h \mod n$, se, e somente se, $t \equiv h \mod k$.*

Demonstração: Primeiro vamos supor que $a^t \equiv a^h \mod n$ e $t \geq h$. Assim podemos escrever: $a^t = a^h a^{t-h}$ e como $a^h \equiv a^t \mod n$, temos que $a^h \equiv a^h a^{t-h} \mod n$. Por outro lado, temos $mdc(a,n) = 1$ o que implica $mdc(a^h, n) = 1$. Portanto, podemos cancelar a^h, nesta última congruência, obtendo $1 \equiv a^{t-h} \mod n$. Daí, pela Proposição 1.2.3, temos que $k|(t-h)$, isto é, $t \equiv h \mod k$. Reciprocamente, se $t \equiv h \mod k$, então, $k|(t-h)$ o que implica que existe $m \in \mathbb{Z}$ tal que $t = h + mk$. Portanto, temos que $a^t \doteq a^{h+mk}$. Por outro lado, como $k = ord_n a$ temos que $a^k \equiv 1 \mod n$. Assim, obtemos $a^t = a^{h+mk} = a^h(a^k)^m \equiv a^h 1^m = a^h \mod n$ como queríamos provar. ■

Corolário 1.2.3 *Se $k = ord_n a$, então os números $1, a, a^2, \ldots, a^{k-1}$ são incongruentes módulo n.*

Demonstração: Suponha que dois destes números sejam congruentes módulo n, isto é, $a^t \equiv a^h \mod n$, onde $t, h \in \{0, 1, 2, \ldots, k-1\}$. Pela Proposição 1.2.4, temos que $t \equiv h \mod k$. Portanto, temos que $k|(t-h)$, mas, como $t, h \in \{0, 1, 2, \ldots, k-1\}$, teremos que $t - h = 0$, isto é, $t = h$. Assim, concluímos que os números $1, a, a^2, \ldots, a^{k-1}$ são todos incongruentes módulo n. ■

Definição 1.2.3 *Quando $ord_n a = \phi(n)$ dizemos que a é uma raiz primitiva módulo n.*

Proposição 1.2.5 *Se a é uma raiz primitiva, então os números $a, a^2, \ldots, a^{\phi(n)}$ formam um sistema reduzido de resíduos módulo n.*

Demonstração: Como a é uma raiz primitiva módulo n temos que $ord_n a = \phi(n)$. Pelo Corolário 1.2.3, sabemos que $1, a, a^2, \ldots, a^{\phi(n)-1}$ são todos incongruentes módulo n. Por outro lado, como $mdc(a,n) = 1$ temos, pela Proposição 1.1.11, que os números $1, a, a^2, \ldots, a^{\phi(n)-1}$ são todos invertíveis em $\mathbb{Z}_n$. Daí formam um sistema

reduzido de resíduos módulo n. Assim, pela Proposição 1.1.12 concluímos que os números $a, a^2, \ldots, a^{\phi(n)}$ formam um sistema reduzido de resíduos módulo n. ■

1.3 Resíduos Quadráticos

Nesta seção estudaremos os resíduos quadráticos, apresentamos o símbolo de Legendre, demonstramos o Critério de Euler e a Lei de Reciprocidade Quadrática, pois, estes resultados serão utilizados nas demonstrações de alguns testes de primalidade estudados no capítulo 2.

Definição 1.3.1 *Sejam $a, n \in \mathbb{N}$, com $n > 1$ e $mdc(a, n) = 1$. Dizemos que a é um* resíduo quadrático *módulo n se a congruência $x^2 \equiv a \mod n$ tiver solução. Caso contrário, dizemos que a não é um resíduo quadrático módulo n ou que a é um resíduo não-quadrático.*

Teorema 1.3.1 *Sejam $a, p \in \mathbb{N}$, com $p > 3$ primo e $1 \leq a \leq p-1$. Caso a congruência $x^2 \equiv a \mod p$ tenha solução, tem exatamente duas soluções incongruentes módulo p.*

Demonstração: Se x_1 é solução da congruência, então $-x_1$ também será solução pois, $(-x_1)^2 = x_1^2$. Além disso, se $x_1 \equiv -x_1 \mod p$ então teríamos $2x_1 \equiv 0 \mod p$ e, como p é ímpar e $p \nmid x_1$ (pois $p \mid (x_1^2 - a)$ e $p \nmid a$), isto é impossível. Precisamos mostrar que só existem essas duas soluções incongruentes. Seja y uma solução de $x^2 \equiv a \mod p$, isto é, $y^2 \equiv a \mod p$. Como x_1 é solução temos $x_1^2 \equiv y^2 \equiv a \mod p$ e, portanto, $x_1^2 - y^2 = (x_1 + y)(x_1 - y) \equiv 0 \mod p$. Logo, $p|(x_1 + y)$ ou $p|(x_1 - y)$, o que implica $y \equiv -x_1 \mod p$ ou $y \equiv x_1 \mod p$. Com isto mostramos que, caso exista uma solução, existem exatamente duas soluções incongruentes. ■

Teorema 1.3.2 (Lagrange) *Seja* $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_2 x^2 + c_1 x + c_0$ *um polinômio com coeficientes naturais tal que* $mdc(c_n, p) = 1$*, em que* p *é primo. Nestas condições a congruência* $f(x) \equiv 0 \mod p$*, tem no máximo* n *soluções incongruentes. É claro que quando* $n > p$ *a congruência acima não tem mais do que* p *soluções distintas módulo* p*.*

Demonstração: A demonstração será feita por indução em n. Para $n = 1$ temos a congruência linear

$$f(x) = c_1 x + c_0 \equiv 0 \mod p.$$

Como $mdc(c_1, p) = 1$ temos que $\overline{c_1}$ é invertível em $\mathbb{Z}_p$, isto é, existe $\overline{x_0} \in \mathbb{Z}_p$ tal que $\overline{c_1 x_0} = \overline{1}$. Daí, temos que $x = x_0(p - c_0)$ é solução de $f(x) = c_1 x + c_0 \equiv 0 \mod p$, de fato, obtemos $f(x_0(p-c_0)) = c_1(x_0(p - c_0)) + c_0 \equiv c_1 x_0 p - c_1 x_0 c_0 + c_0 \equiv p - c_0 + c_0 = p \equiv 0 \mod p$.

Se y_0 também for solução de $f(x) = c_1 x + c_0 \equiv 0 \mod p$, então teremos que $c_1 y_0 + c_0 \equiv c_1(x_0(p - c_0)) + c_0 \mod p$ o que implica $c_1 x_0(p - c_0) \equiv c_1 y_0 \mod p$. Logo, obtemos $x_0(p - c_0) \equiv y_0 \mod p$, isto é, as duas soluções são a mesma módulo p.

Portanto, para $n = 1$ temos exatamente uma solução não congruente módulo n. Logo, o resultado é válido para $n = 1$.

Suponhamos o resultado verdadeiro para todo polinômio de grau menor que n. Devemos mostrar que o resultado seja verdadeiro para todo polinômio de grau n. Suponha, por absurdo, que o número de soluções incongruentes módulo p seja $n+1$. Considere $x_0, x_1, \ldots, x_n$ estas $n + 1$ soluções. É fácil ver que

$$f(x) - f(x_0) = c_n(x^n - x_0^n) + c_{n-1}(x^{n-1} - x_0^{n-1}) + \cdots + c_1(x - x_0) = (x - x_0)h(x),$$

uma vez que $(x^i - x_0^i)$ é divisível por $x - x_0$, para todo $i = 1, 2, \ldots, n$, e que $h(x)$ é um polinômio de grau $n - 1$ tendo c_n como coeficiente de x^{n-1}. Para $k = 1, 2, \ldots, n$

temos que $f(x_k) \equiv f(x_0) \mod p$ (pois, x_k e x_0 são soluções), daí, teremos que $(x_k - x_0)h(x_k) = f(x_k) - f(x_0) \equiv 0 \mod p$. Além disso, temos que $x_k \not\equiv x_0 \mod p$. Portanto, temos que $h(x_k) \equiv 0 \mod p$, isto é, $h(x)$ tem n soluções incongruentes módulo p, contradizendo a hipótese de indução. Logo, $f(x)$ possui no máximo n soluções incongruentes módulo p como queríamos demonstrar. ■

Teorema 1.3.3 *Seja* p *um primo ímpar. Então o conjunto* $\{1, 2, \ldots, p-1\}$ *possui* $\frac{p-1}{2}$ *resíduos quadráticos e* $\frac{p-1}{2}$ *resíduos não-quadráticos.*

Demonstração: Observe que, pelo Teorema 1.3.1, para cada $a \in \{1, 2, \ldots, p-1\}$ se x_1 é solução da congruência $x^2 \equiv a \mod p$, então existe exatamente uma outra solução x_2 que é incongruente à x_1. Sendo assim, formaremos pares de números incongruentes que correspondem a um resíduo quadrático diferente. Além disso, cada número x de 1 até $p-1$ é incongruente com todos os outros números desse intervalo e $p \nmid x^2$ (pois, p é primo e $p \nmid x$), então $\overline{1} \leq \overline{x^2} \leq \overline{p-1}$. Portanto, para cada dois números distintos do conjunto $\{1, 2, \cdots, p-1\}$ teremos um resíduo quadrático distinto. Logo, teremos exatamente $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ resíduos não-quadráticos. ■

Proposição 1.3.1 *Seja* p *um número primo. Então*

$$x^2 \equiv -1 \mod p \text{ possui solução} \quad \Leftrightarrow \quad p = 2 \text{ ou } p \equiv 1 \mod 4.$$

Demonstração: Se $p = 2$ então 1 é solução da congruência. Vamos construir uma solução para o caso $p \equiv 1 \mod 4$.

Para p um primo ímpar podemos escrever o Teorema de Wilson da seguinte forma:

$$(1 \cdot 2 \cdots j \cdots (\tfrac{p-1}{2})(\tfrac{p+1}{2}) \cdots (p-j) \cdots (p-2) \cdot (p-1)) \equiv -1 \mod p$$

Observe que o produto $(p-1)!$ está dividido em duas partes, cada uma com o mesmo número de fatores. Assim, podemos reescrever este produto formando pares, uma vez que para cada fator j na primeira parte temos o fator $(p-j)$ na segunda. Logo, o Teorema de Wilson pode ser escrito como segue

$$\prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv -1 \mod p.$$

Como $j(p-j) \equiv -j^2 \mod p$ temos que

$$\prod_{j=1}^{\frac{p-1}{2}} (-j^2) = (-1)^{\frac{p-1}{2}} \left(\prod_{j=1}^{\frac{p-1}{2}} j \right)^2 \equiv -1 \mod p.$$

Observe que se $p \equiv 1 \mod 4$, então $\frac{p-1}{2}$ é par e, portanto,

$$x = \prod_{j=1}^{\frac{p-1}{2}} j = \left(\frac{p-1}{2} \right)!$$

é uma solução de $x^2 \equiv -1 \mod p$.

Reciprocamente, suponha que a congruência $x^2 \equiv -1 \mod p$ tenha solução e que $p > 2$. Elevando ambos os membros à potência $\frac{p-1}{2}$ obtemos:

$$(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \mod p.$$

Mas, pelo Pequeno Teorema de Fermat, $(x^2)^{\frac{p-1}{2}} = x^{(p-1)} \equiv 1 \mod p$. Assim, temos que $(-1)^{\frac{p-1}{2}} \equiv 1 \mod p$, daí, concluímos que $\frac{p-1}{2}$ é par. Portanto, $p \equiv 1 \mod 4$ como queríamos demonstrar. ■

Definição 1.3.2 *Para p um primo ímpar e a um número natural relativamente primo com p, definimos o Símbolo de Legendre por*

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

Teorema 1.3.4 (Critério de Euler) *Se p for um primo ímpar e a um natural relativamente primo com p, então*

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

Demonstração: Pelo Pequeno Teorema de Fermat temos que $a^{p-1} \equiv 1 \mod p$, assim, teremos $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \mod p$. Como p é primo temos que $p \mid a^{\frac{p-1}{2}} - 1$ ou $p \mid a^{\frac{p-1}{2}} + 1$. Portanto, temos que $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$.

Assim, devemos mostrar que $a^{\frac{p-1}{2}} \equiv 1 \mod p$ se, e somente se, a é um resíduo quadrático módulo p.

Se a é um resíduo quadrático, digamos $a \equiv b^2 \mod p$, com $1 \leq b \leq p-1$, novamente pelo Pequeno Teorema de Fermat temos que $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \mod p$. Por outro lado, o Teorema 1.3.3 nos garante que de 1 até $p-1$ temos exatamente $\frac{p-1}{2}$ resíduos quadráticos módulo p que são soluções incongruentes da congruência $f(x) = x^{\frac{p-1}{2}} - 1 \equiv 0 \mod p$, mas, pelo Teorema 1.3.2, essa congruência possui no máximo $\frac{p-1}{2}$ soluções incongruentes módulo p. Portanto, as soluções incongruentes módulo p de $f(x)$ são exatamente todos os resíduos quadráticos módulo p. Logo, $a^{\frac{p-1}{2}} \equiv 1 \mod p$ se, e somente se, a é um resíduo quadrático módulo p. ■

Iremos agora demonstrar algumas propriedades do símbolo de Legendre que serão utilizadas mais adiante.

Corolário 1.3.1 *O símbolo de Legendre possui as seguintes propriedades:*

1. *Se $a \equiv b \mod p$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. *Se $p \nmid a$, então $\left(\frac{a^2}{p}\right) = 1$.*
3. *$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.*
4. *Se $p \nmid a$ e $p \nmid b$, então $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*

Demonstração: Observe que o item 1 é imediato da definição de congruência e o item 2 segue da definição do Símbolo de Legendre e do fato que a é solução da congruência $x^2 \equiv a^2 \mod p$, isto é, a^2 é resíduo quadrático módulo p. O item 3 segue do Critério de Euler:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p \quad \Rightarrow \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)},$$

pois, $p > 2$ e ambos os lados da congruência são iguais a ± 1. Da mesma forma, aplicando o Critério de Euler temos que

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p,$$

o que mostra que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, pois novamente ambos os lados da congruência são iguais a ± 1. ■

Lema 1.3.1 (Lema de Gauss) *Sejam $p > 2$ um número primo e a um número natural primo relativo com p. Seja s o número de elementos do conjunto*

$$\{a, 2a, 3a, \ldots, \tfrac{p-1}{2}a\}$$

tais que seu resto módulo p é maior do que $\frac{p-1}{2}$. Então

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Demonstração: Como o conjunto $\mathbb{Z}_p^* = \{\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$ temos, pela Proposição 1.1.13, que para cada $j = 1, 2, \ldots, \frac{p-1}{2}$ podemos escrever $aj \equiv \epsilon_j m_j \mod p$ onde $\epsilon_j \in \{-1, 1\}$ e $m_j \in \{1, 2, \ldots, \frac{(p-1)}{2}\}$. Temos que se $i \neq j$ então $m_i \neq m_j$ donde

$$\{m_1, m_2, \ldots, m_{\frac{(p-1)}{2}}\} = \{1, 2, \ldots, \frac{(p-1)}{2}\}.$$

De fato, se $m_i = m_j$ temos $ai \equiv aj \mod p$ ou $ai \equiv -aj \mod p$. Mas, pela Proposição 1.1.11 temos que $a \in \mathbb{Z}_p^*$ e, além disso, temos que $0 < i, j \leq \frac{p-1}{2}$. Portanto, temos que a primeira possibilidade implica $i = j$ e a segunda é impossível. Agora, multiplicando as congruências $aj \equiv \epsilon_j m_j \mod p$, para $j = 1, 2, \ldots, \frac{p-1}{2}$, obtemos

$$a1a2\cdots a\tfrac{p-1}{2} \equiv \epsilon_1\epsilon_2\cdots\epsilon_{\frac{(p-1)}{2}} m_1 m_2\cdots m_{\frac{(p-1)}{2}} \mod p$$

Portanto, temos que $a^{\frac{(p-1)}{2}} 1\cdot 2\cdot\cdots\cdot(\frac{p-1}{2}) \equiv \epsilon_1\epsilon_2\cdots\epsilon_{\frac{(p-1)}{2}} 1\cdot 2\cdot\cdots\cdot(\frac{p-1}{2}) \mod p$. Mas, $1, 2, \ldots, \frac{p-1}{2} \in \mathbb{Z}_p^*$, então temos que $a^{\frac{(p-1)}{2}} \equiv \epsilon_1\epsilon_2\cdots\epsilon_{\frac{(p-1)}{2}} \mod p$. Daí, pelo Critério de Euler teremos que $\left(\frac{a}{p}\right) \equiv \epsilon_1\epsilon_2\cdots\epsilon_{\frac{(p-1)}{2}} \mod p$. Mas, ambos os lados dessa congruência pertencem a $\{-1, 1\}$. Além disso, p é um número primo ímpar, então ambos os lados da congruência são iguais, isto é, $\left(\frac{a}{p}\right) = \epsilon_1\epsilon_2\cdots\epsilon_{\frac{(p-1)}{2}}$. Logo, temos que $\left(\frac{a}{p}\right) = (-1)^s$, em que s é o número de elementos $j \in \{1, 2, \ldots, \frac{p-1}{2}\}$ tais que $\epsilon_j = -1$ (observe que $\epsilon_j = -1$ significa que $aj \equiv \epsilon_j m_j \equiv -m_j \equiv (p - m_j) \mod p$, onde $m_j \in \{1, 2, \ldots, \frac{p-1}{2}\}$, isto é, aj deixa resto maior que $\frac{p-1}{2}$), como queríamos demonstrar. ■

O próximo resultado é chamado *Lei de Reciprocidade Quadrática*. Para p e q primos ímpares, a *Lei de Reciprocidade Quadrática* nos diz que as congruências $x^2 \equiv p \mod q$ e $x^2 \equiv q \mod p$ são ambas solúveis ou ambas insolúveis a menos que p e q sejam congruentes a 3 módulo 4, caso em que uma terá solução e a outra não.

Teorema 1.3.5 (Lei de Reciprocidade Quadrática) .

1. *Se p e q são primos ímpares distintos, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

2. *Se p é um número primo ímpar, então*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} 1, & \text{se } p \equiv \pm 1 \mod 8 \\ -1, & \text{se } p \equiv \pm 3 \mod 8 \end{cases}$$

Demonstração: Para provarmos o item 1 do teorema vamos mostrar que

$$(*) \quad (\tfrac{p-1}{2})(\tfrac{q-1}{2}) = \sum_{1\le i\le \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor$$

e que

$$(**) \quad \left(\frac{p}{q}\right) = (-1)^{r_q} \text{ e } \left(\frac{q}{p}\right) = (-1)^{r_p}, \text{ com } r_q = \sum_{1 \leq i \leq \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor \text{ e } r_p = \sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor$$

Assim, de $(**)$ obtemos $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{r_q}(-1)^{r_p} = (-1)^{r_q + r_p}$ e de $(*)$ temos que $r_q + r_p = \sum_{1 \leq i \leq \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor = (\frac{p-1}{2})(\frac{q-1}{2})$. Portanto, temos que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$ o que demonstra o item 1 do teorema.

Para provarmos a fórmula $(*)$ considere o retângulo de vértices $(0,0), (\frac{p}{2}, 0), (0, \frac{q}{2})$ e $(\frac{p}{2}, \frac{q}{2})$. Assim, teremos que $(\frac{p-1}{2})(\frac{q-1}{2})$ é o número de pontos com ambas as coordenadas inteiras no interior desse retângulo. Por outro lado, observe que a reta $y = i$ intercepta a reta $x = \frac{p}{q}y$ no ponto $(\frac{p}{q}i, i)$ e possui $\lfloor \frac{ip}{q} \rfloor$ pontos com coordenadas inteiras, assim, temos que $\sum_{1 \leq i \leq \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor$ conta o número de tais pontos que estão acima da diagonal $x = \frac{p}{q}y$ do retângulo, além disso, a reta $x = i$ intercepta a reta $x = \frac{p}{q}y$ no ponto $(i, \frac{q}{p}i)$ e possui $\lfloor \frac{iq}{p} \rfloor$ pontos com coordenadas inteiras, logo, $\sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor$ conta o número de tais pontos abaixo desta diagonal (note que como p e q são primos, não há pontos com ambas as coordenadas inteiras na diagonal).

Para mostrar $(**)$, basta verificar que $r_p = \sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \mod 2$, em que s é como no Lema de Gauss aplicado para $a = q$. Pois, nesse caso teremos que s e r_p são ambos pares ou ambos ímpares o que implica $\left(\frac{q}{p}\right) = (-1)^s = (-1)^{r_p}$. E de forma análoga podemos provar que $r_q \equiv s \mod 2$, basta trocar q por p.

Seja r_i o resto da divisão de iq por p, de modo que $iq = \lfloor \frac{iq}{p} \rfloor p + r_i$. Somando e utilizando a notação da demonstração do Lema de Gauss, obtemos

$$q \sum_{1 \leq i \leq \frac{(p-1)}{2}} i = p \sum_{1 \leq i \leq \frac{(p-1)}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{r_i \leq \frac{p}{2}} m_i + \sum_{r_i \geq \frac{p}{2}} (p - m_i).$$

Como $m_i \equiv -m_i \mod 2$, p e q são ímpares temos, módulo 2, que

$$\sum_{1\leq i\leq \frac{p-1}{2}} i \equiv \sum_{1\leq i\leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{r_i\leq \frac{p}{2}} m_i + \sum_{r_i\geq \frac{p}{2}} (1+m_i) \mod 2$$

E como $\{m_1, m_2, \ldots, m_{\frac{(p-1)}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$, concluímos, assim, que

$$\sum_{r_i\leq \frac{p}{2}} m_i + \sum_{r_i\geq \frac{p}{2}} m_i = \sum_{1\leq i\leq \frac{(p-1)}{2}} i \text{ e } \sum_{r_i\geq \frac{p}{2}} 1 = s. \text{ Portanto, teremos que}$$

$$\sum_{1\leq i\leq \frac{(p-1)}{2}} i \equiv \sum_{1\leq i\leq \frac{(p-1)}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{1\leq i\leq \frac{(p-1)}{2}} i + \sum_{r_i\geq \frac{p}{2}} 1 \mod 2.$$

Logo, obtemos $\sum_{1\leq i\leq \frac{(p-1)}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \mod 2$ o que encerra a demonstração do item 1.

Para demonstrarmos o item 2, observe que pelo Critério de Euler temos que $\left(\frac{2}{p}\right) \equiv 2^{\frac{(p-1)}{2}} \mod p$. Assim, primeiro provamos que

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \mod p. \tag{1.3}$$

Como p é um número primo ímpar, temos que deverá ser congruente a 1, 3, 5 ou 7 módulo 8. Vamos analisar cada caso antes de demonstrarmos (1.3).

Quando $p \equiv 1 \mod 8$ temos que existe $k \in \mathbb{Z}$ tal que $p - 1 = 8k$ o que implica $p + 1 = 8k + 2$. Portanto, temos que

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(8k+2)(8k)}{8} = 2k(4k+1).$$

Quando $p \equiv 7 \mod 8$ temos que existe $k \in \mathbb{Z}$ tal que $p - 7 = 8k$ o que implica $p - 1 = 8k + 6$ e $p + 1 = 8k + 8$. Portanto, temos que

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(8k+8)(8k+6)}{8} = 2(k+1)(4k+3).$$

Logo, se $p \equiv \pm 1 \mod 8$ (observe que $-3 \equiv 5 \mod 8$), temos que $\frac{p^2-1}{8}$ é par. Daí, temos $(-1)^{\frac{p^2-1}{8}} = 1$.

Quando $p \equiv 3 \mod 8$ temos que existe $k \in \mathbb{Z}$ tal que $p - 3 = 8k$ o que implica $p - 1 = 8k + 2$ e $p + 1 = 8k + 4$. Portanto, temos que

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(8k+4)(8k+2)}{8} = (2k+1)(4k+1).$$

Quando $p \equiv 5 \mod 8$ temos que existe $k \in \mathbb{Z}$ tal que $p-5 = 8k$ o que implica $p-1 = 8k+4$ e $p+1 = 8k+6$. Portanto, temos que

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(8k+6)(8k+4)}{8} = (4k+3)(2k+1).$$

Logo, se $p \equiv \pm 3 \mod 8$ (observe que $-1 \equiv 7 \mod 8$), temos que $\frac{p^2-1}{8}$ é ímpar. Daí, temos $(-1)^{\frac{p^2-1}{8}} = -1$.

Para provarmos (1.3), consideramos o fato de que para i ímpar, temos $p - i \equiv i(-1)^i \mod p$ e para i par, temos $i \equiv i(-1)^i \mod p$. Portanto, teremos as $\frac{p-1}{2}$ congruências

$$\begin{aligned}
p-1 &\equiv 1(-1)^1 \mod p \\
2 &\equiv 2(-1)^2 \mod p \\
p-3 &\equiv 3(-1)^3 \mod p \\
4 &\equiv 4(-1)^4 \mod p \\
&\vdots \\
t &\equiv \tfrac{p-1}{2}(-1)^{\frac{p-1}{2}} \mod p.
\end{aligned}$$

Caso $\frac{p-1}{2}$ seja par a última congruência acima será

$$t = \frac{p-1}{2} \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \mod p.$$

E, caso $\frac{p-1}{2}$ seja ímpar, a última congruência será

$$t = p - \frac{p-1}{2} \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \mod p.$$

Observe que os números na coluna da esquerda das congruências acima são $2, 4, 6, \ldots, p-1$. Assim, multiplicando todas estas congruências teremos

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{1+2+3+\cdots+\frac{p-1}{2}}(\tfrac{p-1}{2})! \mod p.$$

Observe que

$$2 \cdot 4 \cdot 6 \cdots (p-1) = 2^{\frac{p-1}{2}}(\tfrac{p-1}{2})! \quad \text{e} \quad 1+2+3+\cdots+\tfrac{p-1}{2} = \tfrac{\frac{p-1}{2}(\frac{p-1}{2}+1)}{2} = \tfrac{p^2-1}{8}.$$

Portanto, teremos que

$$2^{\frac{p-1}{2}}(\tfrac{p-1}{2})! \equiv (-1)^{\frac{p^2-1}{8}}(\tfrac{p-1}{2})! \mod p.$$

Como $mdc((\frac{p-1}{2})!, p) = 1$ temos, pela Proposição 1.1.5, que podemos cancelar o termo $(\frac{p-1}{2})!$ em ambos os lados da congruência acima obtendo

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \mod p.$$

O que conclui a demonstração de (1.3).

Como $(\frac{2}{p}) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \mod p$ temos que $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$, pois, p é um número primo ímpar e ambos os membros da última congruência assumem apenas os valores 1 ou -1.

Logo, com os resultados apresentados concluímos a demonstração do item 2 da Lei de Reciprocidade Quadrática. ■

Capítulo 2

Números Primos

Neste capítulo veremos porque o interesse pelos números primos aumentou significativamente nas últimas décadas devido ao seu uso na criptografia RSA. Garantir que um dado número natural é um número primo passou a ter uma importância não puramente acadêmica e passou a ter um valor econômico significativo. Isto porque a segurança do sistema RSA reside na dificuldade de fatorar $n = pq$ quando p e q são primos com mais de 100 algarismos.

2.1 Como Encontrar Números Primos

Para encontrarmos números primos em um dado intervalo escolhemos um número ímpar qualquer desse intervalo e verificamos se este número é primo. Se o número não for primo então escolhemos outro número ímpar qualquer desse intervalo, diferente do anterior, e testamos novamente se esse número é primo. Esse processo deve ser repetido até encontrarmos um número primo.

Portanto, precisamos verificar se o processo de busca pelo nosso número primo descrito acima é viável. Para descobrir isso necessitamos responder a seguinte pergunta: quantos números devemos escolher até encontrarmos um número primo?

Para nos ajudar a responder essa pergunta, iremos enunciar uma definição e um teorema.

Definição 2.1.1 *Dado $x > 0$ um número real. $\pi(x)$ será o número de números primos que são menores ou iguais a x.*

Teorema 2.1.1 (Teorema dos Números Primos) *Dado $x > 0$ um número real. Então*

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{log(x)}} = 1.$$

Demonstração: Uma demonstração pode ser encontrada em [4]. ■

A próxima proposição nos mostra como calcular o número de números primos positivos que são menores ou iguais a um dado número natural. Infelizmente essa fórmula não é muito eficiente para números grandes.

Proposição 2.1.1 *Dado $m > 1$ inteiro. Então*

$$\pi(m) = \sum_{j=2}^{m} \lfloor \frac{(j-1)!+1}{j} - \lfloor \frac{(j-1)!}{j} \rfloor \rfloor$$

é o número de números primos que são menores ou iguais a m.

Demonstração: Se j é um número primo, então pelo Teorema de Wilson, temos $(j-1)! \equiv j-1 \equiv -1 \mod j$. Isto é, $j|[(j-1)!+1]$. Assim, temos que existe $k \in \mathbb{Z}$ tal que $(j-1)!+1 = kj$. Daí, obtemos $k = \frac{(j-1)!+1}{j}$ e $k - \frac{1}{j} = \frac{(j-!)!}{j}$. Portanto, teremos

$$\lfloor \tfrac{(j-1)!+1}{j} - \lfloor \tfrac{(j-1)!}{j} \rfloor \rfloor = \lfloor k - \lfloor k - \tfrac{1}{j} \rfloor \rfloor = \lfloor k - (k-1) \rfloor = 1.$$

Se j não é um número primo e $j > 5$, então pelo Lema 1.2.2 temos que $j|(j-1)!$, isto é, existe $k \in \mathbb{Z}$ tal que $(j-1)! = kj$. Daí, obtemos $k = \frac{(j-1)!}{j}$ e $k + \frac{1}{j} = \frac{(j-1)!+1}{j}$. Logo, teremos

$$\lfloor \frac{(j-1)!+1}{j} - \lfloor \frac{(j-1)!}{j} \rfloor \rfloor = \lfloor k + \frac{1}{j} - k \rfloor = 0.$$

Agora, se $j = 4$, então

$$\lfloor \frac{3!+1}{4} - \lfloor \frac{3!}{4} \rfloor \rfloor = \lfloor \frac{7}{4} - 1 \rfloor = 0.$$

Como as parcelas do somatório da fórmula indicada para $\pi(m)$ é igual a 1 se j é primo e zero se j não é primo temos que este somatório nos dá exatamente o número de números primos que são menores ou iguais a m, como queríamos demonstrar. ■

Por outro lado, o teorema acima nos garante que $\frac{x}{log(x)}$ é uma boa aproximação de $\pi(x)$ quando x for suficientemente grande. Portanto, podemos calcular a probabilidade de que um número x escolhido aleatoriamente seja primo, isto é, $P = \frac{\frac{x}{\log(x)}}{x} = \frac{1}{log(x)}$. Sendo assim, teremos que examinar aproximadamente $\log(x)$ números próximos de x para acharmos um número primo da mesma ordem de grandeza de x. Logo, para encontrarmos um número primo com 100 algarismo, por exemplo, devemos testar $\log(10^{100}) \approx 230$ números aproximadamente. Como não precisamos testar os números pares teremos que testar aproximadamente 115 números. É claro que, como se trata de probabilidade, então esses números são apenas uma média das tentativas reais.

Observe que para $x = 10^2$, por exemplo, temos que $\pi(10^2) = 25$, mas, temos que $\frac{10^2}{log(10^2)} \approx 22$. Isto quer dizer que a diferença entre $\frac{10^2}{log(10^2)}$ e $\pi(10^2)$ é aproximadamente 12% do valor de $\pi(10^2)$, isto é, $\frac{x}{log(x)}$ tem uma margem de erro de aproximadamente 12% do valor de $\pi(x)$. Por outro lado, quando $x = 10^{22}$ temos que $\pi(10^{22}) = 201.467.286.689.315.906.290$ e $\pi(10^{22}) - \frac{10^{22}}{log(10^{22})} = 4.060.704.006.019.620.994$, daí, esse percentual cai para aproximadamente 2%. Portanto, para números com 100 algarismos, isto é, para $x = 10^{100}$, é de se esperar que $\frac{x}{log(x)}$ seja uma boa aproximação de $\pi(x)$.

Como os números que devemos testar são muito grandes temos que é fundamental termos testes de primalidade eficientes e que nos garanta que o número testado

seja realmente um número primo. Na próxima seção iremos explorar alguns dos principais testes de primalidade conhecidos. Como veremos no próximo capítulo a segurança do sistema RSA está intimamente ligada a dificuldade de se fatorar um número muito grande, se o número que escolhermos não for primo teremos que o número que usaremos para o sistema terá um fator primo com pelo menos metade do número de algarismos necessários para garantir a segurança do sistema.

2.2 Teste de Primalidade

A partir da década de 60, apareceram inúmeras tentativas de obter um algoritmo eficiente para o teste de primalidade de um número natural. A importância desse problema vem crescendo muito nos últimos anos devido à utilização crescente de números primos nos algoritmos de criptografia, como os algoritmos RSA e El Gammal. O ponto chave da segurança do sistema de criptografia RSA é a dificuldade de se fatorar um número muito grande. Nos dias de hoje, para que o sistema RSA seja considerado seguro é necessário que o número escolhido para chave contenha dois primos com aproximadamente 100 algarismos cada. Portanto, para escolher esses números gigantes precisamos ter certeza que os números escolhidos sejam realmente primos.

Um algoritmo muito antigo foi criado por Eratóstenes, matemático grego do século III a.C., esse algoritmo é o crivo de Eratóstenes e serve para determinar todos os números primos inferiores a um número n dado arbitrariamente. O crivo consiste em listar todos os números de 2 até n, em seguida retira-se dessa lista todos os múltiplos de cada número primo menor ou igual a raiz quadrada de n, deixando é claro esses primos.

Mostraremos como funciona o processo calculando todos os primos menores que 110. Primeiro escrevemos todos os números de 2 até 110. Como 2 é primo, riscamos

todos os números múltiplos de 2, maiores que 2. Depois, riscamos todos os múltiplos de 3, maiores que 3. Depois, riscamos todos os múltiplos de 5, maiores que 5. E por fim, riscamos todos os múltiplos de 7, maiores que 7. Como o próximo número primo é 11 e $11^2 = 121 > 110$, paramos o processo no número primo 7. Assim, todos os números da lista que não foram riscados são todos os primos menores que 110.

	2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~	~~40~~
41	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	**53**	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~	~~70~~
71	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**	~~80~~
~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~	~~100~~
101	~~102~~	**103**	~~104~~	~~105~~	~~106~~	**107**	~~108~~	**109**	~~110~~

Observe que o crivo de Eratóstenes nos diz que para verificarmos se um dado número n é primo, devemos verificar se esse número é divisível por algum primo menor ou igual que a raiz quadrada de n. O que é muito útil quando n não é um número muito grande. Mas, quando o número é muito grande esse processo demanda muito tempo para sua execução. Portanto, para criptografia RSA esse teste é inútil.

Outro teste de primalidade é o Teorema de Wilson. Mas, devido a dificuldade de se calcular números fatoriais, também, tem um tempo de execução muito longo quando estamos testando números muito grandes. Logo, para o sistema RSA não

serve.

Já o Pequeno Teorema de Fermat se constitui numa ferramenta importante para que possamos verificar se um número é composto sem a necessidade de fatorá-lo. O Teorema de Fermat afirma que: se p é um número primo e a é um número inteiro tal que $mdc(a,p) = 1$, então $a^{p-1} \equiv 1 \mod p$. Portanto, se $mdc(a,n) = 1$ e $a^{n-1} \not\equiv 1 \mod n$, então n é um número composto. Mas, é importante observar que $mdc(1,n) = mdc(n-1,n) = 1$ e $1^{n-1} \equiv (n-1)^{n-1} \equiv 1 \mod n, \forall n \in \mathbb{Z}$ positivo e ímpar, além disso, dado $a \in \mathbb{Z}$, com $mdc(a,n) = 1$, tem-se que $a^{n-1} \equiv b \mod n$, com $0 \leq b < n$. Assim, devemos testar se $b^{n-1} \not\equiv 1 \mod n$ para algum $1 < b < n-1$ para concluir que n é composto.

Será que podemos usar o Pequeno Teorema de Fermat para verificar se um dado número é primo? Isto é, se um número ímpar n que satisfaz $b^{n-1} \equiv 1 \mod n$, para algum $1 < b < n-1$, podemos concluir que n é um número primo? Infelizmente isso não é verdade. Por exemplo, $2^{340} \equiv 1 \mod 341$. Mas, sabemos que $341 = 11 \cdot 31$, é composto. Isto nos leva a seguinte definição.

Definição 2.2.1 *Dizemos que n é pseudoprimo na base a quando é composto e satisfaz $a^{n-1} \equiv 1 \mod n$, com $mdc(a,n) = 1$.*

Usar o Pequeno Teorema de Fermat para determinar se um dado número é primo tem uma boa probalidade de acerto, pois, entre 1 e 10^9 existem 50.847.534 primos, mas apenas 5.597 pseudoprimos para a base 2. Além disso, essa comparação tá levando em conta apenas a base dois. Se testarmos para a base três, por exemplo, temos que $3^{340} \equiv 56 \mod 341$. Portanto, três é uma testemunha de que 341 é um número composto. Temos que há apenas 1.272 pseudoprimos para as bases 2 e 3 entre 1 e 10^9.

Observe que necessitamos analisar apenas as bases a tais que $1 < a < n-1$, isso

nos leva a tentar testar todas as bases nessas condições, mas, isso é impraticável se o número testado é muito grande. Daí, procuramos um processo mais eficiente.

Uma recíproca do Pequeno Teorema de Fermat foi descoberta por Lucas em 1876. Ela será nosso primeiro teste de primalidade.

Proposição 2.2.1 (Teste 1) *Seja $n > 1$ um número inteiro. Suponha que existe um número inteiro $a > 1$ tal que:*

(i) $a^{n-1} \equiv 1 \mod n$,

(ii) $a^m \not\equiv 1 \mod n$, *para* $m = 1, 2, \ldots, n-2$.

Então n é primo.

Demonstração: Primeiro, observe que $a^{n-1} \equiv 1 \mod n$ implica que $\overline{a}$ é invertível em $\mathbb{Z}_n$. Daí, pelo Proposição 1.1.11, temos que $mdc(a, n) = 1$. Assim, pela definição 1.2.2, temos que os itens (1) e (2) nos garantem que $ord_n a = n-1$. Além disso, pelo Teorema de Euler, temos que $a^{\phi(n)} \equiv 1 \mod n$. Mas, sabemos que $\phi(n) \leq n-1$ e pelo Corolário 1.2.2, temos $n-1 = ord_n a | \phi(n)$, então obtemos $\phi(n) = n-1$, isto é, n é um número primo. ■

Apesar de ser conclusivo o teste apresenta dificuldade de implementação para números muito grandes. Em 1891, Lucas reformulou sua recíproca para o Pequeno Teorema de Fermat e apresentou a seguinte proposição.

Proposição 2.2.2 (Teste 2) *Seja $n > 1$ um número inteiro. Suponha que existe um número inteiro $a > 1$ tal que:*

(i) $a^{n-1} \equiv 1 \mod n$,

(ii) $a^m \not\equiv 1 \mod n$, *para todo divisor m de $n-1$.*

Então n é primo.

Demonstração: Basta observar que a Proposição 1.2.3 nos garante que se $a^r \equiv 1 \mod n$, então $ord_n a | r$. Daí, para verificar se $ord_n a = n-1$ é necessário e suficiente verificarmos se $a^m \not\equiv 1 \mod n$, para todo divisor m de $n-1$. Daí, o restante da demonstração segue como foi feita no Teste 1. ■

A princípio parece ser mais fácil a execução desse teste do que o anterior, pois, teríamos que testar um número bem menor de congruências. Mas, sua dificuldade de implementação reside na dificuldade de se conhecer todos os divisores de $n-1$. Em 1967, Brillharte e Selfridge tornaram o teste de Lucas mais flexível.

Proposição 2.2.3 (Teste 3) *Seja $n > 1$ um número inteiro. Supõe-se que, para todo fator primo q de $n-1$, exista um número inteiro $a = a(q) > 1$, tal que:*

(i) $a^{n-1} \equiv 1 \mod n$,

(ii) $a^{\frac{n-1}{q}} \not\equiv 1 \mod n$.

Então n é primo.

Demonstração: Como $\phi(n) \leq n-1$, basta mostrar que $(n-1) | \phi(n)$. Daí, concluímos que $\phi(n) = n-1$, isto é equivalente a dizer que n é um número primo. Sendo assim, suponha que $(n-1) \nmid \phi(n)$. Então existe um número primo q e um número inteiro $r \geq 1$ tais que q^r divide $n-1$, mas, não divide $\phi(n)$.

Sejam $a = a(q)$ e $k = ord_n a$. Como $a^{n-1} \equiv 1 \mod n$ e $a^{\frac{n-1}{q}} \not\equiv 1 \mod n$ temos, pela Proposição 1.2.3, que $k | (n-1)$ e $k \nmid \frac{n-1}{q}$. Logo, temos que $q^r | k$. Por outro lado, o Teorema de Euler nos garante que $a^{\phi(n)} \equiv 1 \mod n$ (lembre que (i) garante que $mdc(a,n) = 1$), então pela Proposição 1.2.3 temos que $k | \phi(n)$. Portanto, chegamos a conclusão que $q^r | \phi(n)$, o que é uma contradição. Logo, temos que $\phi(n) = n-1$, o que é equivalente a dizer que n é um número primo. ■

Na busca por testes de primalidade mais eficientes do ponto de vista computacional e tendo em vista que a maior dificuldade dos primeiros testes reside na dificuldade de se fatorar $n-1$. Foram descobertos testes que supõem somente o conhecimento de fatoração parcial de $n-1$.

O próximo teste foi demonstrado por Pocklington em 1914.

Proposição 2.2.4 (Teste 4) *Seja $n-1 = q^k R$, em que q é um número primo, $k \geq 1$ e q não divide R. Supõe-se a existência de um número inteiro $a > 1$ tal que:*

(i) $a^{n-1} \equiv 1 \mod n$,

(ii) $mdc(a^{\frac{n-1}{q}} - 1, n) = 1$.

Então todo fator primo de n é da forma $mq^k + 1$, com $m \geq 1$.

Demonstração: Se p é um fator primo de n, então p divide n e como, por hipótese, $a^{n-1} \equiv 1 \mod n$ temos que n divide $a^{n-1} - 1$. Portanto, temos que p divide $(a^{n-1} - 1)$, isto é, $a^{n-1} \equiv 1 \mod p$. Além disso, por hipótese, temos que $mdc(a^{\frac{n-1}{q}} - 1, n) = 1$ então p não divide $a^{\frac{n-1}{q}} - 1$. Portanto, pela Proposição 1.2.3 temos que $ord_p a$ divide $n-1$, mas não divide $\frac{n-1}{q}$. Logo, temos que q^k divide a ordem de a módulo p. Por outro lado, o Teorema de Euler nos garante que $a^{p-1} \equiv 1 \mod p$. Daí, temos que $ord_p a$ divide $p-1$. Assim, podemos concluir que q^k divide $p-1$, isto é, existe $m \in \mathbb{Z}$ tal que $p - 1 = mq^k$. Concluímos assim que se p é um fator primo de n, então $p = 1 + mq^k$, para algum $k \geq 1$. ■

Corolário 2.2.1 (Teste 5) *Se $n-1 = FR$, com $F > R$ e para todo fator primo q de F, existe $a > 1$ tal que $a^{n-1} \equiv 1 \mod n$ e $mdc(a^{\frac{n-1}{q}} - 1, n) = 1$. Então, n é primo.*

Demonstração: Seja q um fator primo de F e q^k a maior potência de q que divide F. Assim, pela Proposição anterior todo fator primo de n deve ser da forma $1+mq^k$,

isto é, todo fator primo de n é côngruo a 1 módulo q^k. Como q é um fator primo qualquer de F temos que qualquer fator primo de n é côngruo a 1 módulo F, isto é, todo fator primo de n é da forma $1+tF$ para algum número inteiro $t \geq 1$. Como $F > R$ e $1+tF$ é um fator primo de n temos que $1+tF > \sqrt{n}$, o que é um absurdo. Logo, n é um número primo. ■

Corolário 2.2.2 (Teste 6 - Teste de Pépin) *Seja* $F_n = 2^{2^n}+1$. *Então* F_n *é primo se, e somente se,* $3^{\frac{F_n-1}{2}} \equiv -1 \mod F_n$.

Demonstração: Se $3^{\frac{F_n-1}{2}} \equiv -1 \mod F_n$, então temos que $(3^{\frac{F_n-1}{2}})^2 \equiv (-1)^2 \mod F_n$, isto é, $3^{F_n-1} \equiv 1 \mod F_n$. Além disso, 2 é o único fator primo que divide $F_n - 1$ e como $3^{\frac{F_n-1}{2}} \equiv -1 \mod F_n$ podemos concluir que todas as hipóteses da Proposição 2.2.3 estão satisfeitas. Logo, F_n é um número primo. Reciprocamente, se F_n é um número primo, então pelo Critério de Euler temos que

$$3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \mod F_n.$$

Além disso, pela Lei de Reciprocidade Quadrática, temos que

$$(\tfrac{3}{F_n})(\tfrac{F_n}{3}) = (-1)^{(\frac{3-1}{2})(\frac{F_n-1}{2})} = 1, \text{ isto é, temos que } (\tfrac{3}{F_n}) = (\tfrac{F_n}{3}).$$

Observe que $F_n = 2^{2^n}+1 \equiv 2 \mod 3$. De fato, provaremos por indução em n. Para $n = 1$, temos $2^{2^1}+1 = 5 \equiv 2 \mod 3$. Portanto, para $n = 1$ a congruência está verificada.

Suponha que a congruência seja válida para $n = k$. Então basta provar que vale para $n = k+1$. Observe que, $2^{2^{k+1}}+1 = 2^{2\cdot 2^k}+1 = 2^{2^k}\cdot 2^{2^k}+1 = (2^{2^k}-1)\cdot 2^{2^k}+2^{2^k}+1$. Como, por hipótese de indução, $2^{2^k}+1 \equiv 2 \mod 3$ temos que $2^{2^k}-1 \equiv 0 \mod 3$. Portanto, temos que $2^{2^{k+1}}+1 = (2^{2^k}-1)\cdot 2^{2^k}+2^{2^k}+1 \equiv 2 \mod 3$.

Logo, pelo princípio de indução, temos que $F_n = 2^{2^n}+1 \equiv 2 \mod 3$. Daí, pelo Corolário 1.3.1 item 1 temos que $(\frac{F_n}{3}) = (\frac{2}{3})$. Mas, pelo item 2 da Lei de

Reciprocidade Quadrática, obtemos $(\frac{2}{3}) = -1$. Logo, podemos concluir que $3^{\frac{F_n-1}{2}} \equiv (\frac{3}{F_n}) = (\frac{F_n}{3}) = (\frac{2}{3}) = -1 \mod F_n$ como queríamos demonstrar. ■

Teorema 2.2.1 (Teste 7 - Proth (1878)) *Seja $n = h \cdot 2^k + 1$, com $2^k > h$. Então n é um número primo se, e somente se, existe um inteiro a com $a^{\frac{n-1}{2}} \equiv -1 \mod n$.*

Demonstração: Se n é um número primo, então podemos tomar a qualquer com $\left(\frac{a}{n}\right) = -1$, pois, pelo Teorema 1.3.3 metade dos inteiros entre 1 e $n-1$ serve como a. Além disso, pelo Critério de Euler, temos que $(\frac{a}{n}) \equiv a^{\frac{n-1}{2}} \mod n$. Assim, podemos concluir que existe um inteiro a com $a^{\frac{n-1}{2}} \equiv -1 \mod n$. Reciprocamente, tome $F = 2^k$ e observe que $a^{\frac{n-1}{2}} \equiv -1 \mod n$ implica que $n | a^{\frac{n-1}{2}} + 1$, isto é, todo fator primo de n divide $a^{\frac{n-1}{2}} + 1$, daí, nenhum fator primo de n divide $a^{\frac{n-1}{2}} + 1 - 2 = a^{\frac{n-1}{2}} - 1$ (pois, tal fator dividiria 2, mas, n é ímpar). Portanto, $mdc(a^{\frac{n-1}{2}} - 1, n) = 1$. Por outro lado, $a^{\frac{n-1}{2}} \equiv -1 \mod n$ implica que $(a^{\frac{n-1}{2}})^2 \equiv (-1)^2 \mod n$, isto é, $a^{n-1} \equiv 1 \mod n$. Assim, pelo Corolário 2.2.1, temos que n é primo. ■

A grande maioria dos 100 maiores primos conhecidos estão nas condições do teorema de Proth, segundo [4]. Isto acontece porque primos desta forma são mais frequentes e sua primalidade é facilmente demonstrada usando este teste.

O próximo teorema justifica a aplicação de um algoritmo utilizado atualmente para determinar se um dado número é primo. Com este algoritmo é possível determinar com certeza absoluta se um dado número é primo. Todos os algoritmos que tomavam por fundamento os testes anteriores davam apenas uma probabilidade de que o número testado seria um número primo, claro que, essa probabilidade era bem alta, mas, não se tinha garantia absoluta de que o número testado seria um número primo.

A demonstração desse teorema utiliza resultados matemáticos que foge ao objetivo deste trabalho, por esse motivo não faremos sua demonstração aqui. Mas, quem

desejar estudar um pouco mais o assunto recomendamos [4], onde pode ser vista uma demonstração desse teorema e todos os resultados utilizados nessa demonstração.

Teorema 2.2.2 (Teste 8 - AKSL) *Sejam $N, r, v \in \mathbb{Z}$, maiores que 1. Seja S um conjunto finito com s elementos. Suponha que:*

1. *N e r são primos relativos e $v = ord_r N$.*
2. *$mdc(N, a - b) = 1$, para quaisquer elementos $a, b \in S$, com $a \neq b$.*
3. *$\binom{s+t-1}{s} \geq N\sqrt{\frac{t}{2}}$, para todo t divisor de $\phi(r)$ que seja múltiplo de v.*
4. *$(x + a)^N \equiv x^N + a \mod (x^r - 1, N)$, para todo $a \in S$.*

Então N é potência de um número primo.

Capítulo 3

Criptografia RSA

Neste capítulo iremos estudar o funcionamento da criptografia RSA. A criptografia de chave pública RSA foi desenvolvida por R. L. Rivest, A. Shamir e L. Adleman em 1978. Observe que as iniciais dos nomes dos autores deram origem ao nome do código.

Como veremos neste capítulo a segurança da criptografia RSA reside na dificuldade de fatorar um número grande (número com pelo menos 231 algarismos) em seus fatores primos.

3.1 Criptossistemas Simétricos e Assimétricos

A palavra *criptografia* tem origem no grego, *cryptos* significa oculto, secreto e *grapho* significa escrita. Assim, criptografia é o estudo de métodos que permitam escrever mensagens em cifras ou códigos, de modo que apenas os legítimos destinatários sejam capazes de decodificar e ler as mensagens.

Um dos mais simples exemplos de criptografia consiste em transladar o alfabeto em um certo número de vezes, por exemplo, fazer a primeira letra assumir a posição da terceira, a segunda assumir a posição da quarta, e assim por diante, até que

a penúltima ocupa a posição da primeira e a última ocupa a posição da segunda. Um código semelhante a esse foi usado pelo imperador romano Júlio Cesar para se comunicar com suas tropas em combate pela Europa.

Um criptossistema é um conjunto de procedimentos que torna possível a criptografia. Todo sistema criptográfico consiste basicamente dos seguintes elementos:

1. Um alfabeto.
2. A mensagem original.
3. A chave de codificação.
4. O procedimento ou função de codificação.
5. A mensagem codificada.
6. A chave de decodificação.
7. O procedimento ou função de decodificação.

Quando a chave ou a função de decodificação é facilmente deduzida da chave ou função de codificação será necessário manter tal chave em sigilo, sendo conhecida apenas pelos usuários legítimos do criptossistema. Neste caso, o sistema é dito *criptossistema simétrico* ou de *chave secreta*. O cifrário de Cesar é um exemplo de criptossistema simétrico. Uma desvantagem desse tipo de sistema é que se o número de usuário for grande o sistema perde a segurança, pois, a chave secreta passa a ser de conhecimento de todos os usuários do sistema. Por isso, esse tipo de sistema é recomendado apenas quando o número de usuário não excede a dois.

O criptossistema de chave pública é caracterizado pelo fato de ser muito difícil obter a chave de decodificação a partir da chave de codificação, daí, o sistema é dito *criptossistema assimétrico* ou de *chave pública*. Esse tipo de criptossistema foi

proposto em 1976 por W. Diffie e M. E. Hellman da Universidade de Stanford e, independentemente, por R. C. Merkle da Universidade da California. O criptossistema de chave pública possui uma chave de codificação pública, de conhecimento de todos e uma chave de decodificação secreta, de conhecimento apenas do receptor da mensagem. Neste tipo de sistema criptográfico vários receptores podem manter comunicação com vários transmissores diferentes. Isto é possível porque cada transmissor e cada receptor possui uma chave de codificação e uma chave de decodificação.

Para entender melhor como a comunicação entre várias pessoas acontece, vamos supor que n pessoas estão usando um determinado criptossistema de chave pública. Vamos representar uma pessoa qualquer que esteja usando esse criptossistema, por u_i, com $i = 1, 2, \ldots, n$. Logo, se um usuário u_i deseja mandar uma mensagem para um usuário u_j, então o usuário u_i codifica a mensagem com a chave pública do usuário u_j. Assim, quando o usuário u_j receber a mensagem será capaz de decodificá-la através de sua chave secreta de decodificação.

Observe que a chave de codificação de qualquer usuário é pública, então qualquer pessoa pode mandar uma mensagem para outro usuário desse sistema, além disso, cada usuário do sistema possui sua própria chave de decodificação que nesse caso é conhecida apenas por ele, garantindo assim que a segurança do sistema independa do número de usuários desse sistema. E, isso realmente é muito vantajoso, pois, com as novas tecnologias, principalmente, a internet, temos uma comunicação entre um número cada vez maior de pessoas. Assim, ter um sistema que admita um número qualquer de usuários sem comprometer a segurança do sistema é sem dúvida uma grande vantagem. E, isso torna os criptossistemas de chave pública a única opção conhecida no momento para transmissão de mensagens com a máxima segurança possível.

Nas próximas seções mostraremos todos os passos que devem ser seguidos para quem deseja utilizar o sistema RSA, inclusive mostrando os fundamentos matemáticos que justificam porque o sistema funciona.

3.2 Geração das Chaves

Nesta seção descreveremos como obter as chaves de codificação e decodificação do criptossistema RSA.

Para gerar a chave de codificação na criptografia RSA cada usuário escolhe dois números primos, p e q, distintos e extremamente grandes. A diferença entre esses números primos não pode ser pequena, daí, a escolha de um número com 104 e outro com 127 algarismos, respectivamente, nos garante uma enorme distância entre os dois números primos escolhidos, dificultando assim a fatoração do número $n = pq$.

Depois da escolha dos números primos, calculamos

$$n = pq$$

e

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

Em seguida, escolhemos um número $t \in \mathbb{Z}$, $1 < t < \phi(n)$, tal que $mdc(t, \phi(n)) = 1$.

Obtemos assim a chave de codificação $k_c = (t, n)$.

E, para obter a chave de decodificação determinamos $r \in \mathbb{Z}$, $0 < r < \phi(n)$, tal que $tr \equiv 1 \mod \phi(n)$, ou seja, r é o inverso multiplicativo de t módulo $\phi(n)$.

Obtemos assim a chave de decodificação $k_d = (r, n)$.

Agora o usuário divulga a chave de codificação $k_c = (t, n)$ e mantém em segredo a chave de decodificação $k_d = (r, n)$. Como foi dito na seção anterior cada usuário deve proceder como descrito acima para obter suas chaves de codificação e de decodificação.

3.3 Codificação e Decodificação

Primeiramente, a mensagem é convertida em uma sequência numérica, através de uma correspondência biunívoca entre os símbolos usados na mensagem original e um subconjunto finito de $\mathbb{N}$. Esta etapa chamaremos de pré-codificação, para distingui-la da codificação propriamente dita.

Essa sequência numérica é quebrada em blocos m de números naturais, onde $1 \leq m < n$. A escolha dos blocos não é única, mas certos cuidados devem ser tomados. Tais como:

1. Não devemos escolher blocos que comecem por zero, pois, perderíamos informação ao codificar a mensagem e não teríamos como corrigir um erro na decodificação a partir desse bloco.

2. Não escolher blocos que correspondam a alguma unidade linguística, como palavra, letra ou qualquer outra, pois, isso facilitaria a quebra do código.

Depois, cada bloco m é codificado como segue

$$k_c(m) \equiv m^t \mod n.$$

Note que $k_c(m)$ é o resto da divisão euclidiana de m^t por n.

E, finalmente, a decodificação de $k_c(m)$ será

$$k_d(k_c(m)) \equiv (k_c(m))^r \mod n.$$

Note que $k_d(k_c(m))$ é o resto da divisão euclidiana de $(m^t)^r = m^{tr}$ por n.

Observe que após a mensagem ser separada em blocos para a codificação, esses blocos devem permanecer separados e mantidos na mesma ordem em que foram formados a partir da mensagem original. Depois, da decodificação de todos os blocos, estes devem ser reunidos novamente obedecendo a ordem estebelecida anteriormente para obter a mensagem original.

Portanto, a criptografia RSA tem como alfabeto de entrada um alfabeto numérico e os blocos que constituem a mensagem são elementos do conjunto $\mathbb{Z}_n$. Na última seção deste capítulo apresentaremos dois exemplos para tornar a teoria mais clara.

É fácil ver porque a decodificação do RSA funciona. De fato, seja $k_c(m) \equiv m^t \mod n$ a codificação de um bloco m. Queremos mostrar que $k_d(k_c(m)) \equiv m \mod n$.

Primeiro mostraremos que $k_d(k_c(m)) \equiv m \mod p$.

Como $tr \equiv 1 \mod \phi(n)$ temos que existe $i \in \mathbb{N}$ tal que $tr = 1 + i\phi(n)$.

Se $mdc(m,p) = 1$, usando o Pequeno Teorema de Fermat temos que $m^{p-1} \equiv 1 \mod p$, daí, elevando ambos os membro dessa congruência ao expoente $i(q-1)$, obtemos $(m^{p-1})^{i(q-1)} = m^{i(p-1)(q-1)} \equiv 1 \mod p$, assim, multiplicando ambos os membros dessa última congruência por m obtemos, $m^{1+i(p-1)(q-1)} \equiv m \mod p$. Mas, $1 + i(p-1)(q-1) = 1 + i\phi(n) = tr$. Logo, temos que $k_d(k_c(m)) \equiv m^{tr} = m^{1+i(p-1)(q-1)} \equiv m \mod p$.

Se $mdc(m,p) = p$, então esta última congruência é verdadeira, pois, ambos os lados é congruente a zero módulo p. Assim, teremos $k_d(k_c(m)) \equiv m \mod p$ para qualquer bloco m da mensagem original.

De modo, análogo encontramos $k_d(k_c(m)) = (m^t)^r = m^{tr} \equiv m \mod q$.

Observe que $k_d(k_c(m)) \equiv m \mod p$ e $k_d(k_c(m)) \equiv m \mod q$ implicam que

$p|[k_d(k_c(m)) - m]$ e $q|[k_d(k_c(m)) - m]$. Como p e q são primos temos que $n = pq|[k_d(k_c(m)) - m]$, isto é,

$$k_d(k_c(m)) \equiv m \mod n.$$

Como vimos a matemática que justifica o sistema de RSA é bem simples. E para garantir a segurança do sistema, é necessário que os números primos escolhidos sejam grandes. Consequentemente o número n terá sua decomposição em fatores primos computacionalmente inviável. É nessa escolha que reside a necessidade de uma matemática mais sofisticada, como vimos no capítulo anterior.

3.4 Segurança do RSA

Um ponto fundamental para a segurança da criptografia RSA refere-se à escolha adequada dos primos p e q. Assim, para dificultar a fatoração de n a nossa escolha deve obedecer aos seguintes parâmetros:

1. Os números primos p e q não podem ser próximos um do outro. Suponha que n tenha a algarismos. Então para costruir n, escolha um primo p entre $\frac{4a}{10}$ e $\frac{45a}{100}$ algarismos e, em seguida, escolha um primo q próximo de $\frac{10^a}{p}$ algarismos.

2. Além disso, precisamos ter certeza que os números $p-1$, $q-1$, $p+1$ e $q+1$ possuem fatores primos grandes.

3. E, também, devemos ter $mdc(p-1, q-1)$ pequeno.

Veremos como é possível quebrar o código RSA. Isto é, como decodificar a mensagem conhecendo apenas a chave pública do sistema.

Observe que a chave de codificação $k_c = (t, n)$ é a chave pública, isto é, qualquer usuário conhece. Portanto, uma forma de quebrar o código RSA seria calcular r

conhecendo apenas t e n. Mas, como vimos na Seção 2, r é o inverso multiplicativo de t módulo $\phi(n)$. Portanto, seria necessário calcular $\phi(n)$. Mas, temos que $n = pq$, em que p e q são números primos, então obtemos $\phi(n) = (p-1)(q-1)$. Isto é, devemos conhecer a fatoração de n.

Outra forma de quebrar o código RSA seria calcular a raiz t-ésima de m^t módulo n. Porém sabemos que este problema é computacionalmente inviável guando n é grande.

Portanto, para conseguir quebrar o código do RSA é necessário fatorar n ou calcular a raiz t-ésima de m^t módulo n. Mas, até o momento não se conhece um algoritmo eficiente que consiga resolver um desses problemas com a tecnologia atual. Logo, o sistema RSA tem se mostrado seguro.

3.5 Assinatura Digital

Uma característica importante do sistema RSA é que $k_d(k_c(m)) = k_c(k_d(m))$, isto é, k_d e k_c comutam. De fato, temos que $k_c(m) \equiv m^t \mod n$. Daí, teremos que $k_d(k_c(m)) \equiv (m^t)^r = m^{tr} = (m^r)^t \equiv k_c(k_d(m)) \mod n$.

Esta propriedade possibilita enviarmos mensagens com "assinaturas digitais". Vejamos como isso funciona.

Suponha que um usuário i deseja enviar uma mensagem m assinada para um usuário j. Então o usuário i usa sua chave secreta $k_{d,i}(m)$, depois usa a chave pública do usuário j $k_{c,j}(k_{d,i}(m))$ e envia esta para j.

Para que o usuário j possa ler a mensagem deve proceder da seguinte forma: aplica a sua chave secreta $k_{d,j}$ e depois aplica a chave pública do usuário i $k_{c,i}$, daí, obtem a mensagem original m.

Observe que dessa forma o usuário j pode ter certeza que foi de fato o usuário i quem mandou a mensagem m, pois, a chave $k_{d,i}$ usada no processo é conhecida apenas pelo usuário i.

Severino Coller Coutinho no seu livro *Números Inteiros e Criptografia RSA* descreve como um especialista em segurança de computadores descobriu um método para "quebrar"o código RSA.

> Recentemente descobiu-se que o uso pouco cuidadoso da técnica de autenticação de assinaturas torna vulneráveis certos métodos de chave pública como o RSA. No final de 1995, um consultor em assuntos de segurança de computadores (mas formado em biologia!) descobriu que é possível usar o sistema de assinaturas para quebrar o RSA. O método consiste em enviar uma mensagem assinada e marcar o tempo que o sistema leva para confirmar a assinatura. Fazendo isto para mensagens de tamanhos ligeiramente diferentes, é possível obter informações suficientes para encontrar a chave de decodificação do sistema RSA que esteja sendo usado. Portanto, a segurança do RSA não depende exclusivamente da nossa capacidade de inventar novos algoritmos de fatoração. Há muitos outros fatores importantes, que não têm um caráter puramente matemático.

3.6 Aplicação

Nos exemplos abaixo iremos usar o número 99 para representar o espaço em branco entre as palavras e a correspondência entre o alfabeto $\mathbb{F} = \{A, B, C, \ldots, Z\}$ e o conjunto $\{10, 11, 12, \ldots, 35\}$, como segue abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Antes de começarmos com os exemplos, vamos provar uma afirmação que nos garante a validez dos cálculos realizados para codificar e decodificar as mensagens. Essa afirmação nos diz que dada uma potência qualquer em uma congruência módulo n, podemos substituir a base da potência pelo resto da divisão euclidiana dessa base por n.

Afirmação 1 *Dados a, b, t e n números naturais, com $n > 1$ e $0 \leq b < n$. Então* $(an + b)^r \equiv b^r \mod n$.

Demonstração: Basta observar que $(an + b)^r = (an)^r + k_{r-1}(an)^{r-1}b + \cdots + k_1(an)b^{r-1} + b^r \equiv 0 + 0 + \cdots + 0 + b^r = b^r \mod n$. ■

Exemplo 3.6.1 *Vamos codificar e decodificar, pelo método RSA, a mensagem "BOA NOITE". Sabendo que $n = 7597$, $t = 4947$ e $\phi(n) = 7420$.*

Solução: Assim, devemos transformar a mensagem em uma sequência numérica através da correspondência dada no início dessa Seção. Portanto a mensagem será 112410992324182914.

Em seguida quebramos esse número nos seguintes blocos: $112 - 4109 - 923 - 241 - 82 - 914$.

Vamos agora codificar a mensagem.

$k_c(112) \equiv 112^{4947} = 112 \cdot (112^2)^{2473} = 112 \cdot 12544^{2473} \equiv 112 \cdot 4947 \cdot (4947^2)^{1236} = 554064 \cdot 24472809^{1236} \equiv 7080 \cdot (2872^2)^{618} = 7080 \cdot 8248384^{618} \equiv 7080 \cdot (5639^2)^{309} =$

$7080 \cdot 31798321^{309} \equiv 7080 \cdot 4876 \cdot (4876^2)^{154} = 34522080 \cdot 23775376^{154} \equiv 1312 \cdot (4363^2)^{77} = 1312 \cdot 19035769^{77} \equiv 1312 \cdot 5284 \cdot (5284^2)^{38} = 6932608 \cdot 27920656^{38} \equiv 4144 \cdot (1681^2)^{19} = 4144 \cdot 2825761^{19} \equiv 4144 \cdot 7274 \cdot (7274^2)^9 = 30143456 \cdot 52911076^9 \equiv 6157 \cdot 5568 \cdot (5568^2)^4 = 34282176 \cdot 31002624^4 \equiv 4512 \cdot (6864^2)^2 = 4512 \cdot 47114496^2 \equiv 4512 \cdot 5499^2 = 4512 \cdot 30239001 \equiv 4512 \cdot 2941 = 13269792 \equiv 5430 \mod 7597.$

$k_c(4109) \equiv 4109^{4947} = 4109 \cdot (4109^2)^{2473} = 4109 \cdot 16883881^{2473} \equiv 4109 \cdot 3347 \cdot (3347^2)^{1236} = 13752823 \cdot 11202409^{1236} \equiv 2253 \cdot (4431^2)^{618} = 2253 \cdot 19633761^{618} \equiv 2253 \cdot (3113^2)^{309} = 2253 \cdot 9690769^{309} \equiv 2253 \cdot 4594 \cdot (4594^2)^{154} = 10350282 \cdot 21104836^{154} \equiv 3168 \cdot (370^2)^{77} = 3168 \cdot 136900^{77} \equiv 3168 \cdot 154^2 \cdot (154^3)^{25} = 75132288 \cdot 3652264^{25} \equiv 5555 \cdot 5704 \cdot (5704^2)^{12} = 31685720 \cdot 32535616^{12} \equiv 6230 \cdot (5262^2)^6 = 6230 \cdot 27688644^6 \equiv 6230 \cdot (5176^2)^3 = 6230 \cdot 26790976^3 \equiv 6230 \cdot 3954 \cdot 3954^2 = 24633420 \cdot 15634116 \equiv 3946 \cdot 7087 = 27965302 \equiv 745 \mod 7597.$

$k_c(923) \equiv 923^{4947} = 923 \cdot (923^2)^{2473} = 923 \cdot 851929^{2473} \equiv 923 \cdot 1065 \cdot (1065^2)^{1236} = 982995 \cdot 1134225^{1236} \equiv 2982 \cdot (2272^2)^{618} = 2982 \cdot 5161984^{618} \equiv 2982 \cdot (3621^2)^{309} = 2982 \cdot 13111641^{309} \equiv 2982 \cdot 6816 \cdot (6816^2)^{154} = 20325312 \cdot 46457856^{154} \equiv 3337 \cdot (2201^2)^{77} = 3337 \cdot 4844401^{77} \equiv 3337 \cdot 5112 \cdot (5112^2)^{38} = 17058744 \cdot 26132544^{38} \equiv 3479 \cdot (6461^2)^{19} = 3479 \cdot 41744521^{19} \equiv 3479 \cdot 6603 \cdot (6603^2)^9 = 22971837 \cdot 43599609^9 \equiv 6106 \cdot 426 \cdot (426^2)^4 = 2601156 \cdot 181476^4 \equiv 2982 \cdot (6745^2)^2 = 2982 \cdot 45495025^2 \equiv 2982 \cdot 4189^2 = 2982 \cdot 17547721 \equiv 2982 \cdot 6248 = 18631536 \equiv 3692 \mod 7597.$

$k_c(241) \equiv 241^{4947} = (241^3)^{1649} = 13997521^{1649} \equiv 3847 \cdot (3847^2)^{824} = 3847 \cdot 14799409^{824} \equiv 3847 \cdot (453^2)^{412} = 3847 \cdot 205209^{412} \equiv 3847 \cdot (90^4)^{103} = 3847 \cdot 65610000^{103} \equiv 3847 \cdot 2308 \cdot (2308^2)^{51} = 8878876 \cdot 5326864^{51} \equiv 5580 \cdot 1367 \cdot (1367^2)^{25} = 7627860 \cdot 1868689^{25} \equiv 472 \cdot 7424 \cdot (7424^2)^{12} = 3504128 \cdot 55115776^{12} \equiv 1911 \cdot (7138^2)^6 = 1911 \cdot 50951044^6 \equiv 1911 \cdot (5562^2)^3 = 1911 \cdot 30935844^3 \equiv 1911 \cdot 860 \cdot 860^2 = 1643460 \cdot 739600 \equiv 2508 \cdot 2691 = 6749028 \equiv 2892 \mod 7597.$

$k_c(82) \equiv 82^{4947} = (82^3)^{1649} = 551368^{1649} \equiv 4384 \cdot (4384^2)^{824} = 4384 \cdot 19219456^{824} \equiv 4384 \cdot (6643^2)412 = 4384 \cdot 44129449^{412} \equiv 4384 \cdot (6073^2)^{206} = 4384 \cdot 36881329^{206} \equiv 4384 \cdot (5491^2)^{103} = 4384 \cdot 30151081^{103} \equiv 4384 \cdot 6185 \cdot (6185^2)^{51} = 27115040 \cdot 38254225^{51} \equiv 1347 \cdot 3330 \cdot (3330^2)^{25} = 4485510 \cdot 11088900^{25} \equiv 3280 \cdot 4877 \cdot (4877^2)^{12} = 15996560 \cdot 23785129^{12} \equiv 4875 \cdot (6519^2)^6 = 4875 \cdot 42497361^6 \equiv 4875 \cdot (7340^2)^3 = 4875 \cdot 53875600^3 \equiv 4875 \cdot 5273 \cdot 5273^2 = 25705875 \cdot 27804529 \equiv 5224 \cdot 7106 = 37121744 \equiv 2802 \mod 7597.$

$k_c(914) \equiv 914^{4947} = 914 \cdot (914^2)^{2473} = 914 \cdot 835396^{2473} \equiv 914 \cdot 7323 \cdot (7323^2)^{1236} = 6693222 \cdot 53626329^{1236} \equiv 265 \cdot (6703^2)^{618} = 265 \cdot 44930209^{618} \equiv 265 \cdot (1551^2)^{309} = 265 \cdot 2405601^{309} \equiv 265 \cdot 4949 \cdot (4949^2)^{154} = 1311485 \cdot 24492601^{154} \equiv 4801 \cdot (7470^2)^{77} = 4801 \cdot 55800900^{77} \equiv 4801 \cdot 935^2 \cdot (935^3)^{25} = 4197154225 \cdot 817400375^{25} \equiv 1650 \cdot 1160 \cdot (1160^2)^{12} = 1914000 \cdot 1345600^{12} \equiv 7153 \cdot (931^3)^4 = 7153 \cdot 806954491^4 \equiv 7153 \cdot (1151^2)^2 = 7153 \cdot 1324801^2 \equiv 7153 \cdot 2923^2 = 7153 \cdot 8543929 \equiv 7153 \cdot 4901 = 35056853 \equiv 4295 \mod 7597.$

Portanto, a mensagem codificada tem a seguinte seguência de blocos: $5430 - 745 - 3692 - 2892 - 4295$. Próximo passo, encontrar a chave de decodificação. Isto é, encontrar r tal que $4947r \equiv 1 \mod 7420$. Daí, concluímos que $\exists i \in \mathbb{Z}$ tal que $4947r - 7420i = 1$.

Assim devemos aplicar o algoritmo de Euclides para determinar o máximo divisor comum de 4947 e 7420. Portanto, teremos

- $2473 = 7420 - 4947$
- $1 = 4947 - 2 \cdot 2473$

Daí, temos que

$$1 = 4947 - 2 \cdot 2473 = 4947 - 2 \cdot (7420 - 4947) = 3 \cdot 4947 - 2 \cdot 7420.$$

Logo, obtemos $r = 3$, assim, a chave de decodificação é $k_d = (3, 7597)$. Agora calculamos $k_d(5430), k_d(745), k_d(3692), k_d(2892), k_d(2802)$ e $k_d(4295)$.

$k_d(5430) \equiv 5430^3 = 5430 \cdot 5430^2 = 5430 \cdot 29484900 = 5430 \cdot (7597 \cdot 3881 + 943) \equiv 5430 \cdot 943 = 5120490 = 7597 \cdot 674 + 112 \equiv 112 \mod 7597.$

$k_d(745) \equiv 745^3 = 745 \cdot 745^2 = 745 \cdot 555025 = 745 \cdot (7597 \cdot 73 + 444) \equiv 745 \cdot 444 = 330780 = 7597 \cdot 43 + 4109 \equiv 4109 \mod 7597.$

$k_d(3692) \equiv 3692^3 = 3692 \cdot 3692^2 = 3692 \cdot 13630864 = 3692 \cdot (7597 \cdot 1794 + 1846) \equiv 3692 \cdot 1846 = 6815432 = 7597 \cdot 897 + 923 \equiv 923 \mod 7597.$

$k_d(2892) \equiv 2892^3 = 2892 \cdot 2892^2 = 2892 \cdot 8363664 = 2892 \cdot (7597 \cdot 1100 + 6964) \equiv 2892 \cdot 6964 = 20139888 = 7597 \cdot 2651 + 241 \equiv 241 \mod 7597.$

$k_d(2802) \equiv 2802^3 = 2802 \cdot 2802^2 = 2802 \cdot 7851204 = 2802 \cdot (7597 \cdot 1033 + 3503) \equiv 2802 \cdot 3503 = 9815406 = 7597 \cdot 1292 + 82 \equiv 82 \mod 7597.$

$k_d(4295) \equiv 4295^3 = 4295 \cdot 4295^2 = 4295 \cdot 18447025 = 4295 \cdot (7597 \cdot 2428 + 1509) \equiv 4295 \cdot 1509 = 6481155 = 7597 \cdot 853 + 914 \equiv 914 \mod 7597.$

Portanto, a mensagem original é $112 - 4109 - 923 - 241 - 82 - 914$, isto é, $11 - 24 - 10 - 99 - 23 - 24 - 18 - 29 - 14$, que significa BOA NOITE. ■

Exemplo 3.6.2 *A chave pública utilizada pelo Banco de Toulouse para codificar suas mensagens é a seguinte:* $n = 10403$ *e* $t = 8743$. *Recentemente os computadores do banco receberam, de local indeterminado, a seguinte mensagem:*

$$4746 - 8214 - 9372 - 9009 - 4453 - 8198$$

O que diz a mensagem mandada ao Banco de Toulouse?

Solução: Para resolver esse problema devemos fatorar 10403 para obtermos $\phi(n)$. Para isso, iremos usar o algoritmo de Fermat.

Seja $a_1 = \lfloor\sqrt{10403}\rfloor = 101$. Como $a_1^2 \neq n$ temos que tomamos $a_2 = a_1 + 1 = 102$ e calculamos $s_1 = \sqrt{a_2^2 - n} = 1$. Logo, temos que $n = (a_2 + s_1)(a_2 - s_1) = 103 \cdot 101$. Portanto, temos que $\phi(10403) = 102 \cdot 100 = 10200$.

Queremos calcular $r \in \mathbb{Z}$ tal que $8743r \equiv 1 \mod 10200$. Assim, devemos aplicar o algoritmo de Euclides para determinar o $mdc(8743, 10200)$. Portanto, teremos

- $1457 = 10200 - 8743$
- $1 = 8743 - 6 \cdot 1457$

Daí, obtemos

$$1 = 8743 - 6 \cdot (10200 - 8743) = 7 \cdot 8743 - 6 \cdot 10200.$$

Portanto, obtemos $r = 7$, assim, temos que a chave de decodificação é $k_d = (7, 10403)$.

Agora podemos decifrar a mensagem

$k_d(4746) \equiv 4746^7 = 4746 \cdot (4746^2)^3 \equiv 4746 \cdot 2021^3 = 4746 \cdot 2021 \cdot 2021^2 \equiv 100 \cdot 6465 \equiv 1514 \mod 10403$

$k_d(8214) \equiv 8214^7 = 8214 \cdot (8214^2)^3 \equiv 8214 \cdot 6341^3 = 8214 \cdot 6341 \cdot 6341^2 \equiv 7556 \cdot 686 \equiv 2722 \mod 10403$

$k_d(9372) \equiv 9372^7 = 9372 \cdot (9372^2)^3 \equiv 9372 \cdot 1855^3 = 9372 \cdot 1855 \cdot 1855^2 \equiv 1647 \cdot 8035 \equiv 1029 \mod 10403$

$k_d(9009) \equiv 9009^7 = 9009 \cdot (9009^2)^3 \equiv 9009 \cdot 8278^3 = 9009 \cdot 8278 \cdot 8278^2 \equiv 7798 \cdot 723 \equiv 9931 \mod 10403$

$k_d(4453) \equiv 4453^7 = 4453 \cdot (4453^2)^3 \equiv 4453 \cdot 1091^3 = 4453 \cdot 1091 \cdot 1091^2 \equiv 22 \cdot 4339 \equiv 1831 \mod 10403$

$k_d(8198) \equiv 8198^7 = 8198 \cdot (8198^2)^3 \equiv 8198 \cdot 3824^3 = 8198 \cdot 3824 \cdot 3824^2 \equiv 4913 \cdot 6761 \equiv 14 \mod 10403$.

Portanto, a mensagem recebida pelo banco foi $1514 - 2722 - 1029 - 9931 - 1831 - 14$, isto é, $15 - 14 - 27 - 22 - 10 - 29 - 99 - 31 - 18 - 31 - 14$ que significa FERMAT VIVE. ■

Capítulo 4

Criptografia RSA no Ensino Médio

Neste capítulo iremos abordar a criptografia RSA numa linguagem que seja possível um aluno do ensino médio entender e aplicar esse criptossistema. Primeiro mostaremos a matemática necessária para a implementação do sistema. Num segundo momento, mostraremos como funciona o sistema, através de dois exemplos.

4.1 Matemática Básica

Como já vimos no capítulo anterior a base para a criptografia RSA está na aritmética dos restos. Portanto, necessitaremos calcular o resto da divisão euclidiana. O aluno aprende a usar o algoritmo da divisão euclidiana desde o quarto ano do ensino fudamental. Mas, para implementar o RSA são necessários muitos cálculos, assim, aconcelhamos o uso de uma calculadora, caso contrário, o processo poderá ser muito moroso.

4.1.1 Divisão Euclidiana

Iremos ilustrar com um exemplo como proceder para encontrar o resto da divisão euclidiana usando uma calculadora simples. Imagine que você queira saber quanto

é o resto da divisão de 2013 por 13. Para isso iremos executar três passos:

1. Divida 2013 por 13, isto é, $\frac{2013}{13} = 154,846....$

2. Multiplica 154 por 13, isto é, $154 \cdot 13 = 2002$.

3. O resto procurado é a diferença entre 2013 e 2002, isto é, $r = 2013 - 2002 = 11$.

Esse procedimento para encontrar o resto da divisão tem sua justificativa formal no seguinte teorema.

Teorema 4.1.1 (Algoritmo da Divisão Euclidiana) *Sejam a e b dois números naturais com $0 < a < b$. Nestas condições, existem únicos q e r números naturais tais que*

$$b = aq + r, \text{ com } 0 \leq r < a.$$

Esse Teorema foi demonstrado por Euclides, matemático grego do século III a.C., por isso é chamado algoritmo da divisão euclidiana. Com esse Teorema Euclides provou que o procedimento que fizemos acima para encontrar o resto da divisão euclidiana de 2013 por 13 é sempre possível ser repetido para quaisquer dois números naturais.

4.1.2 Máximo Divisor Comum

O procedimento para calcular o máximo divisor comum de dois números descrito abaixo era apresentado nos livros do sexto ano do ensino fundamental na década de 1980, hoje caiu no esquecimento. Mais uma vez iremos ilustrar com um exemplo, como calcular o máximo divisor comum de 2013 e 13, procedendo da seguinte forma:

1. Divida 2013 por 13, isto é, $\frac{2013}{13} = 154,846....$

2. Escreva $11 = 2013 - 154 \cdot 13$.

3. Divida 13 por 11, isto é $\frac{13}{11} = 1,1818....$

4. Escreva $2 = 13 - 1 \cdot 11$.

5. Divida 11 por 2, isto é, $\frac{11}{2} = 5,5$.

6. Escreva $1 = 11 - 5 \cdot 2$.

7. Como 2 dividido por 1 deixa resto zero, temos que o máximo divisor comum de 2013 e 13 é 1.

Além disso, devemos escrever o máximo divisor comum encontrado como combinação linear de 2013 e 13, isto é, será necessário encontrarmos dois números naturais, t e s, tais que $1 = 2013t - 13s$ ou $1 = 13s - 2013t$. Para isso procederemos da seguinte forma:

1. Partindo da última igualdade temos $1 = 11 - 5 \cdot 2$.

2. Substituindo $2 = 13 - 1 \cdot 11$ na igualdade acima obtemos $1 = 11 - 5 \cdot (13 - 1 \cdot 11) = 11 - 5 \cdot 13 + 5 \cdot 11 = 6 \cdot 11 - 5 \cdot 13$.

3. Substituindo $11 = 2013 - 154 \cdot 13$ na última igualdade acima obtemos $1 = 6 \cdot (2013 - 154 \cdot 13) - 5 \cdot 13 = 6 \cdot 2013 - 929 \cdot 13$.

4. Daí, obtemos $t = 6$ e $s = 929$.

4.1.3 Congruência

Pela Definição 1.1.1 apresentada no Capítulo 1, temos que $2013 \equiv 13 \mod 100$, pois, o resto da divisão euclidiana de 2013 por 100 é 13.

Uma consequência imediata da definição de congruência e do algoritmo da divisão euclidiana é que, dado qualquer número natural a, esse número será congruente módulo n a um único número natural b tal que $0 \leq b < n$.

Vejamos como calcular a seguinte potência $37^{44} \equiv x \mod 120$, então procedemos como segue:

1. Escrevemos $37^{44} = (37^2)^{22}$
2. Calculamos $37^2 = 1369$ e tomamos o resto da divisão euclidiana por 120, isto é, $1369 - 11 \cdot 120 = 49$.
3. Escrevemos $(37^2)^{22} = 1369^{22} \equiv 49^{22} = (49^2)^{11} \mod 120$
4. Calculamos $49^2 = 2401$ e tomamos o resto da divisão euclidiana por 120, isto é, $2401 - 20 \cdot 120 = 1$.
5. Escrevemos $37^{44} = (37^2)^{22} = 1369^{22} \equiv 49^{22} = (49^2)^{11} = 2401^{11} \equiv 1^{11} = 1 \mod 120$. Logo, temos que $37^{44} \equiv 1 \mod 120$.

Estamos preparados para implementar o sistema RSA. Aqui abordamos toda a matemática necessária na implementação do sistema RSA. É claro que a matemática que garante o funcionamento do sistema, bem como a matemática que garante sua segurança é bem mais sofisticada e foi parcialmente abordada nos capítulos 1 e 2 deste trabalho.

4.2 Criptografia RSA

Nos exemplos abaixo iremos usar o número 99 para representar o espaço em branco entre as palavras e a correspondência entre o alfabeto $\mathbb{F} = \{A, B, C, \ldots, Z\}$ e o conjunto $\{10, 11, 12, \ldots, 35\}$, como segue abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Iremos ilustrar com dois exemplos, o funcionamento do sistema RSA.

Exemplo 4.2.1 *Queremos codificar e decodificar a seguinte mensagem: SEJA FELIZ.*

Solução: Vamos transformar a mensagem em uma sequência numérica através da correspondência dada no início dessa Seção, onde o número 10 corresponde a letra A, por exemplo. Portanto a mensagem será 28141910991514211835.

Para chave de codificação vamos escolher $n = 11 \cdot 13 = 143$ e $t = 77$. Assim, temos que $k_c = (77, 143)$ é a chave de codificação que iremos usar.

Como $\phi(143) = (11-1)(13-1) = 120$ devemos quebrar o número que forma a mensagem em blocos de modo que cada bloco m, com $1 < m < \phi(143) = 120$, seja diferente de qualquer unidade linguística. Assim, uma possível quebra seria: $2 - 81 - 41 - 9 - 109 - 91 - 51 - 42 - 11 - 83 - 5$.

Vamos agora codificar a mensagem original.

$k_c(2) = 2^{77} = (2^{11})^7 = 2048^7 \equiv 46^7 = 46 \cdot (46^2)^3 = 46 \cdot 2116^3 \equiv 46 \cdot 114^3 = 46 \cdot 114 \cdot 114^2 = 5244 \cdot 12996 \equiv 96 \cdot 126 = 12096 \equiv 84 \mod 143$.

$k_c(81) = 81^{77} = 81 \cdot (81^2)^{38} = 81 \cdot 6561^{38} \equiv 81 \cdot 126^{38} = 81 \cdot (126^2)^{19} = 81 \cdot 15876^{19} \equiv 81 \cdot 3^{19} = 81 \cdot 3 \cdot (3^6)^3 = 243 \cdot 729^3 \equiv 100 \cdot 14^3 = 1400 \cdot 196 \equiv 113 \cdot 53 = 5989 \equiv 126 \mod 143$.

$k_c(41) = 41^{77} = 41 \cdot (41^2)^{38} = 41 \cdot 1681^{38} \equiv 41 \cdot (108^2)^{19} = 41 \cdot 11664^{19} \equiv 41 \cdot 81 \cdot (81^2)^9 = 3321 \cdot 6561^9 \equiv 32 \cdot 126 \cdot (126^2)^4 = 4032 \cdot 15876^4 = 28 \cdot 3^4 = 2268 \equiv 123 \mod 143$.

$k_c(9) = 9^{77} = 9^2 \cdot (9^3)^{25} = 81 \cdot 729^{25} \equiv 81 \cdot 14 \cdot (14^2)^{12} = 1134 \cdot 196^{12} \equiv 133 \cdot (53^2)^6 = 133 \cdot 2809^6 \equiv 133 \cdot 92^6 = 133 \cdot (92^2)^3 = 133 \cdot 8464^3 \equiv 133 \cdot 27^3 = 133 \cdot 27 \cdot 27^2 = 3591 \cdot 729 \equiv 16 \cdot 14 = 224 \equiv 81 \mod 143.$

$k_c(109) = 109^{77} = 109 \cdot (109^2)^{38} = 109 \cdot 11881^{38} \equiv 109 \cdot (12^2)^{19} = 109 \cdot 144^{19} \equiv 109 \cdot 1^{19} = 109 \mod 143$

$k_c(91) = 91^{77} = 91 \cdot (91^2)^{38} = 91 \cdot 8281^{38} \equiv 91 \cdot (130^2)^{19} = 91 \cdot 16900^{19} \equiv 91 \cdot 26 \cdot (26^2)^9 = 2366 \cdot 676^9 \equiv 78 \cdot 104 \cdot (104^2)^4 = 8112 \cdot 10816^4 \equiv 104 \cdot 91^4 = 104 \cdot (91^2)^2 = 104 \cdot 8281^2 \equiv 104 \cdot 130^2 = 1757600 \equiv 130 \mod 143.$

$k_c(51) = 51^{77} = 51 \cdot (51^2)^{38} = 51 \cdot 2601^{38} \equiv 51 \cdot (27^2)^{19} = 51 \cdot 729^{19} \equiv 51 \cdot 14 \cdot (14^2)^9 = 714 \cdot 196^9 \equiv 142 \cdot 53 \cdot (53^2)^4 = 7526 \cdot 2809^4 \equiv 90 \cdot (92^2)^2 = 90 \cdot 8464^2 \equiv 90 \cdot 27^2 = 65610 \equiv 116 \mod 143.$

$k_c(42) = 42^{77} = 42 \cdot (42^2)^{38} = 42 \cdot 1764^{38} \equiv 42 \cdot (48^2)^{19} = 42 \cdot 2304^{19} \equiv 42 \cdot 16 \cdot (16^2)^9 = 672 \cdot 256^9 \equiv 100 \cdot 113 \cdot (113^2)^4 = 11300 \cdot 12769^4 \equiv 3 \cdot (42^2)^2 = 3 \cdot 1764^2 \equiv 3 \cdot 48^2 = 6912 \equiv 48 \mod 143.$

$k_c(11) = 11^{77} = 11^2 \cdot (11^3)^{25} = 121 \cdot 1331^{25} \equiv 121 \cdot 44 \cdot (44^2)^{12} = 5324 \cdot 1936^{12} \equiv 33 \cdot (77^2)^6 = 33 \cdot 5929^6 \equiv 33 \cdot (66^2)^3 = 33 \cdot 4356^3 \equiv 33 \cdot 66 \cdot 66^2 = 2178 \cdot 4356 \equiv 33 \cdot 66 = \equiv 33 \mod 143.$

$k_c(83) = 83^{77} = 83 \cdot (83^2)^{38} = 83 \cdot 6889^{38} \equiv 83 \cdot (25^2)^{19} = 83 \cdot 625^{19} \equiv 83 \cdot 53 \cdot (53^2)^9 = 4399 \cdot 2809^9 \equiv 109 \cdot 92 \cdot (92^2)^4 = 10028 \cdot 8464^4 \equiv 18 \cdot (27^2)^2 = 18 \cdot 729^2 \equiv 18 \cdot 14^2 = 3528 \equiv 96 \mod 143.$

$k_c(5) = 5^{77} = 5 \cdot (5^4)^{19} = 5 \cdot 625^{19} \equiv 5 \cdot 53 \cdot (53^2)^9 = 265 \cdot 2809^9 = 122 \cdot 92 \cdot (92^2)^4 = 11224 \cdot 8464^4 \equiv 70 \cdot (27^2)^2 = 70 \cdot 14^2 = 13720 \equiv 135 \mod 143.$

Portanto, a mensagem codificada tem a seguinte sequência de blocos: $84 - 126 - 123 - 81 - 109 - 130 - 116 - 48 - 33 - 96 - 135$. Próximo passo encontrar a chave

de decodificação.

Como $\phi(n) = (11-1)\cdot(13-1) = 120$ devemos encontrar um número natural r, tal que $77r \equiv 1 \mod 120$, isto é, $77r - 120i = 1$, para algum $i \in \mathbb{N}$. Assim, devemos calcular o $mdc(77, 120)$.

- $43 = 120 - 77$
- $34 = 77 - 43$
- $9 = 43 - 34$
- $7 = 34 - 3 \cdot 9$
- $2 = 9 - 7$
- $1 = 7 - 3 \cdot 2$

Fazendo sucessivas substituições nas igualdades acima e percorrendo o sentido de baixo para cima, obtemos o seguinte resultado:

- $1 = 7 - 3 \cdot (9 - 7) = 7 - 3 \cdot 9 + 3 \cdot 7 = 4 \cdot 7 - 3 \cdot 9$
- $= 4 \cdot (34 - 3 \cdot 9) - 3 \cdot 9 = 4 \cdot 34 - 15 \cdot 9$
- $= 4 \cdot 34 - 15 \cdot (43 - 34) = 19 \cdot 34 - 15 \cdot 43$
- $= 19 \cdot (77 - 43) - 15 \cdot 43 = 19 \cdot 77 - 34 \cdot 43$
- $= 19 \cdot 77 - 34 \cdot (120 - 77) = 53 \cdot 77 - 34 \cdot 120.$

Portanto, obtemos $1 = 53 \cdot 77 - 34 \cdot 120$, isto é, $r = 53$. Logo, temos que $k_d = (53, 143)$ é a chave de decodificação.

Vamos agora decodificar os blocos: $84-126-123-81-109-130-116-48-33-96-135$. Se nossos cálculos estiverem certos devemos encontrar como resultado a seguinte sequência: $2-81-41-9-109-91-42-11-83-5$.

$k_d(84) = 84^{53} = 84 \cdot (84^2)^{26} = 84 \cdot 7056^{26} \equiv 84 \cdot (49^2)^{13} = 84 \cdot 2401^{13} \equiv 84 \cdot 113 \cdot (113^2)^6 = 9492 \cdot 12769^6 \equiv 54 \cdot (42^2)^3 = 54 \cdot 1764^3 \equiv 54 \cdot 48 \cdot 48^2 = 2592 \cdot 2304 \equiv 18 \cdot 16 = 288 \equiv 2 \mod 143.$

$k_d(126) = 126^{53} = 126 \cdot (126^2)^{26} = 126 \cdot 15876^{26} \equiv 126 \cdot 3^2 \cdot (3^6)^4 = 1134 \cdot 729^4 \equiv 133 \cdot (14^2)^2 = 133 \cdot 196^2 \equiv 133 \cdot 53^2 = 373597 \equiv 81 \mod 143.$

$k_d(123) = 123^{53} = 123 \cdot (123^2)^{26} = 123 \cdot 15129^{26} \equiv 123 \cdot (114^2)^{13} = 123 \cdot 12996^{13} \equiv 123 \cdot 126 \cdot (126^2)^6 = 15498 \cdot 15876^6 \equiv 54 \cdot 3^6 = 39366 \equiv 41 \mod 143.$

$k_d(81) = 81^{53} = 81 \cdot (81^2)^{26} = 81 \cdot 6561^{26} \equiv 81 \cdot (126^2)^{13} = 81 \cdot 15876^{13} \equiv 81 \cdot 3^6 \cdot 3^7 = 59049 \cdot 2187 \equiv 133 \cdot 42 = 5586 \equiv 9 \mod 143.$

$k_d(109) = 109^{53} = 109 \cdot (109^2)^{26} = 109 \cdot 11881^{26} \equiv 109 \cdot (12^2)^{13} = 109 \cdot 144^{13} \equiv 109 \cdot 1^{13} = 109 \mod 143.$

$k_d(130) = 130^{53} = 130 \cdot (130^2)^{26} = 130 \cdot 16900^{26} \equiv 130 \cdot (26^2)^{13} = 130 \cdot 676^{13} \equiv 130 \cdot 104 \cdot (104^2)^6 = 13520 \cdot 10816^6 \equiv 78 \cdot (91^2)^3 = 78 \cdot 8281^3 \equiv 78 \cdot 130 \cdot 130^2 = 10140 \cdot 16900 \equiv 130 \cdot 26 = 3380 \equiv 91 \mod 143.$

$k_d(116) = 116^{53} = 116 \cdot (116^2)^{26} = 116 \cdot 13456^{26} \equiv 116 \cdot (14^2)^{13} = 116 \cdot 53 \cdot (53^2)^6 = 6148 \cdot 2809^6 \equiv 142 \cdot (92^2)^3 = 142 \cdot 8464^3 \equiv 142 \cdot 27 \cdot 27^2 = 3834 \cdot 729 \equiv 116 \cdot 14 = 1624 \equiv 51 \mod 143.$

$k_d(48) = 48^{53} = 48 \cdot (48^2)^{26} = 48 \cdot 2304^{26} \equiv 48 \cdot (16^2)^{13} = 48 \cdot 256^{13} \equiv 48 \cdot 113 \cdot (113^2)^6 = 5424 \cdot 12769^6 \equiv 133 \cdot (42^2)^3 = 133 \cdot 1764^3 \equiv 133 \cdot 48 \cdot 48^2 = 6384 \cdot 2304 \equiv 92 \cdot 16 = 1472 \equiv 42 \mod 143.$

$k_d(33) = 33^{53} = 33 \cdot (33^2)^{26} = 33 \cdot 1089^{26} \equiv 33 \cdot (88^2)^{13} = 33 \cdot 774413 \equiv 33 \cdot 22 \cdot (22^2)^6 = 726 \cdot 484^6 \equiv 11 \cdot (55^2)^3 = 11 \cdot 3025^3 \equiv 11 \cdot 22 \cdot 22^2 = 242 \cdot 484 \equiv 99 \cdot 55 = 5445 \equiv 11 \mod 143.$

$k_d(96) = 96^{53} = 96 \cdot (96^2)^{26} = 96 \cdot 9216^{26} \equiv 96 \cdot (64^2)^{13} = 96 \cdot 409613 \equiv 96 \cdot 92 \cdot (92^2)^6 = 8832 \cdot 8464^6 \equiv 109 \cdot (27^2)^3 = 109 \cdot 729^3 \equiv 109 \cdot 14 \cdot 14^2 = 1526 \cdot 196 \equiv 96 \cdot 53 = 5088 \equiv 83 \mod 143.$

$k_d(135) = 135^{53} = 135 \cdot (135^2)^{26} = 135 \cdot 18225^{26} \equiv 135 \cdot (64^2)^{13} = 135 \cdot 4096^{13} \equiv 135 \cdot 92 \cdot (92^2)^6 = 12420 \cdot 8464^6 \equiv 122 \cdot (27^2)^3 = 122 \cdot 729^3 \equiv 122 \cdot 14 \cdot 14^2 = 1708 \cdot 196 \equiv 135 \cdot 53 = 7155 \equiv 5 \mod 143.$

Portanto, a mensagem decodificada tem a seguinte sequência de blocos: $2-81-41-9-109-91-51-42-11-83-5$. Assim, a mensagem original é formada pelas dezenas: $28-14-19-10-99-15-14-21-18-35$, que após aplicarmos a correspondência dada no início dessa Seção obtemos a frase: SEJA FELIZ. ■

Exemplo 4.2.2 *A mensagem* $51-307-269-365-71-158$ *foi codificada pelo sistema RSA usando chave* $k_c = (169, 391)$. *Sabendo que* $\phi(391) = 352$ *decodifique a mensagem.*

Solução: Devemos encontrar $a, b \in \mathbb{N}$ tais que $352a - 169b = 1$.

- $14 = 352 - 2 \cdot 169$
- $1 = 169 - 12 \cdot 14$

Portanto, obtemos $1 = 169 - 12 \cdot (352 - 2 \cdot 169) = 25 \cdot 169 - 12 \cdot 352$. Isto é, $b = 25$. Logo, temos que $k_d = (25, 391)$ é a chave de decodificação. Vamos decodificar a mensagem $51-307-269-365-71-158$.

$k_d(51) = 51^{25} = 51 \cdot (51^3)^8 = 51 \cdot 132651^8 \equiv 51 \cdot (102^2)^4 = 51 \cdot 10404^4 \equiv 51 \cdot (238^2)^2 = 51 \cdot 56644^2 \equiv 51 \cdot 340^2 = 51 \cdot 115600 \equiv 51 \cdot 255 = 13005 \equiv 102 \mod 391.$

$k_d(307) = 307^{25} = 307 \cdot (307^2)^{12} = 307 \cdot 94249^{12} \equiv 307 \cdot (18^4)^3 = 307 \cdot 104976^3 \equiv 307 \cdot 188 \cdot 188^2 = 57716 \cdot 35344 \equiv 239 \cdot 154 = 36806 \equiv 52 \mod 391.$

$k_d(269) = 269^{25} = 269 \cdot (269^2)^{12} = 269 \cdot 72361^{12} \equiv 269 \cdot (26^3)^4 = 269 \cdot 17576^4 \equiv 269 \cdot (372^2)^2 = 269 \cdot 138384^2 \equiv 269 \cdot 361^2 = 269 \cdot 130321 \equiv 269 \cdot 118 = 31742 \equiv 71 \mod 391.$

$k_d(365) = 365^{25} = 365 \cdot (365^2)^{12} = 365 \cdot 133225^{12} \equiv 365 \cdot (285^2)^6 = 365 \cdot 81225^6 \equiv 365 \cdot (288^2)^3 = 365 \cdot 82944^3 \equiv 365 \cdot 52^3 = 365 \cdot 140608 \equiv 365 \cdot 239 = 87235 \equiv 42 \mod 391.$

$k_d(71) = 71^{25} = 71 \cdot (71^3)^8 = 71 \cdot 357911^8 \equiv 71 \cdot (146^2)^4 = 71 \cdot 21316^4 \equiv 71 \cdot (202^2)^2 = 71 \cdot 40804^2 \equiv 71 \cdot 140^2 = 71 \cdot 19600 \equiv 71 \cdot 50 = 3550 \equiv 31 \mod 391.$

$k_d(158) = 158^{25} = 158 \cdot (158^2)^{12} = 158 \cdot 24964^{12} \equiv 158 \cdot (331^2)^6 = 158 \cdot 109561^6 \equiv 158 \cdot (81^3)^2 = 158 \cdot 531441^2 \equiv 158 \cdot 72^2 = 819072 \equiv 318 \mod 391.$

Portanto, a mensagem decodificada tem a seguinte sequência de blocos: $102 - 52 - 71 - 42 - 31 - 318$. Assim, a mensagem original é formada pelas dezenas: $10 - 25 - 27 - 14 - 23 - 13 - 18$, que após aplicarmos a correspondência dada no início dessa Seção obtemos a frase: APRENDI. ■

Referências Bibliográficas

[1] Ribenboim, P., *Números Primo. Velhos Mistérios e Novos Recordes*, 1 ed. Rio de Janeiro: IMPA 328 pp. (2012).

[2] Coutinho, S. C., *Números Inteiros e Criptografia RSA*, 2 ed. Rio de Janeiro: IMPA 226 pp. (2011).

[3] Hefez, A., *Elementos de Aritmética*, 2 ed. Rio de Janeiro: IMPA 169 pp. (2006).

[4] Martinez, F. B., Moreira, C. G., Tengan, E., *Teoria dos Números: Um Passeio Com Primos e Outros Números Familiares Pelo Mundo Inteiro*, 1 ed. Rio de Janeiro: IMPA 450pp (Projeto Euclides). (2010).

[5] Gonçalves, A., *Introdução à Álgebra*, 5 ed. Rio de Janeiro: IMPA 194 pp (Projeto Euclides). (2006)

[6] Santos J. P. O., *Introdução à Teoria dos Números*, 3 ed. Rio de Janeiro: IMPA 198 pp (Coleção Matemática Universitária). (2010).

[7] Silva, A. de A. e, *Números, Relações e Criptografia*, Texto usado pelo autor na disciplina Matemática Elementar na UFPB, 186pp.

[8] Souza, B. A., *Teoria dos Números e o RSA*, Dissertação de Mestrado apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, (2004).