VIVIAN DA SILVEIRA MIRANDA

EXPLORANDO OS NÚMEROS PRIMOS E UMA DAS SUAS APLICAÇÕES ATUAIS: A CRIPTOGRAFIA

2020

VIVIAN DA SILVEIRA MIRANDA

EXPLORANDO OS NÚMEROS PRIMOS E UMA DAS SUAS APLICAÇÕES ATUAIS: A CRIPTOGRAFIA

Dissertação apresentada à Universidade Federal de Lavras, como parte das exigências do Programa de Pós-Graduação do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT - UFLA, para a obtenção do título de Mestre.

Adriana Xavier Freitas

Orientadora

2020

Ficha catalográfica elaborada pelo Sistema de Geração de Ficha Catalográfica da Biblioteca Universitária da UFLA, com dados informados pelo(a) próprio(a) autor(a).

Miranda, Vivian da Silveira
Explorando os números primos e uma das suas aplicações atuais: a criptografia / Vivian da Silveira Miranda. – Lavras : UFLA, 2020.
90 p. :

Dissertação (mestrado profissional)–Universidade Federal de Lavras, 2020.
Orientadora: Adriana Xavier Freitas.
Bibliografia.

1. Números primos. 2. Criptografia. 3. Ensino médio. I. Xavier, Adriana Freitas. II. Título.

Dedico esta monografia ao meu marido e à minha mãe que estiveram ao meu lado me dando apoio e me incentivando de forma paciente e carinhosa.

AGRADECIMENTOS

Agradeço, em primeiro lugar, a Deus por ter me capacitado, me dado determinação e, principalemte, por ter me protegido durante todo o mestrado. Agradeço também aos meus colegas, que não poderiam ser melhores! Sempre prontos a ajudar e incentivar. Em especial à Karina que foi minha companheira de estrada e amiga para dividir os momentos bons e aflitos que passamos nesse tempo. Aos meus professores que sempre procuraram a melhor forma de nos transmitir um pouco do que sabem. E por último, agradeço à minha querida orientadora Adriana que me guiou pelo melhor caminho para desenvolver esta dissertação, sempre com muito carinho nas palavras e com explicações claras e concisas.

"A matemática é o alfabeto com o qual Deus escreveu o universo". Galileu Galilei

RESUMO

Os números primos são um grande mistério na Matemática, com grandes questionamentos e curiosidades sobre eles. Será que existe um função que nos fornece todos os números primos? Como saber se um determinado número é primo ou não? Qual a utilidade dos números primos? Perguntas como essas nos motivou a escrever sobre esse tema pouco discutido na educação básica e de tamanha importância, principalmente nos dias de hoje. Uma de suas aplicações, que tem influência direta no nosso dia a dia, é na criptografia. Quando fazemos uma transação bancária, mandamos uma mensagem ou até mesmo escrevemos um bilhete em códigos, estamos usando a criptografia e consequentemente a Matemática. Esta dissertação aborda, em um primeiro momento, conceitos sobre números primos, funções que os geram, testes de primalidades, primos especiais e alguns teoremas fundamentais sobre eles. Em seguida, são abordadas as criptografias RSA e ElGamal, sua codificação e decodificação bem como suas autenticidades. Também será apresentado o Protocolo Diffie-Hellman, um avanço na troca de chaves. Por último são propostas atividades para despertar o interesse dos alunos dos anos finais do Ensino Fundamental e do Ensino Médio e reforçar a importância da Matemática na vida de todos.

Palavras-chave: Números primos. Criptografia. Ensino Médio.

ABSTRACT

Prime numbers are a great mystery in Mathematics with many questions and curiosities about them. Is there a function which give us all prime numbers? How can one know wether a given number is prime or not? How useful are prime numbers? Questions like those motivated us to write about this topic which is not so much discussed in basic education and has huge relevance, especially nowadays. One of its applications with direct influence in everyday life is encryption. When we make a bank transaction, exchange a message or even when we write a note using codes, we are using encryption and consequently Mathematics. In this dissertation we work, first, with concepts about prime numbers, generating functions, primality tests, special primes and some fundamental theorems about them. Next, we present RSA and ElGamal encryption systems, including their encoding, decryption and authenticity. We also present the Diffie-Hellman Protocol, an advance in key exchange. Lastly, we suggest activities to arouse the interest of students of basic education and to reinforce the importance of Mathematics in the life of everybody.

Keywords: Prime number. Encryption. High school.

SUMÁRIO

1 INTRODUÇÃO

Constantemente os professores são cobrados para que os conteúdos ministrados sejam contextualizados e despertem o interesse em seus alunos. A Matemática apresenta uma vantagem, pois praticamente tudo que vamos fazer em nosso dia a dia, seja explicita ou implicitamente, envolve cálculos, raciocínio lógico, equações, proporções ou conceitos da geometria. Até mesmo mandar uma mensagem, algo que parece não ter absolutamente nada a ver com a Matemática, pode conter cálculos e propriedades matemáticas. Com certeza ao enviar uma mensagem ou uma informação, você se deparou com a seguinte mensagem: “As mensagens e as chamadas são protegidas com a criptografia de ponta a ponta”. E é sobre essa segurança que iremos trabalhar nessa dissertação. Estudaremos sobre a CRIPTOGRAFIA, ciência de transformar, através de um processo conhecido como chave, uma informação de sua forma original em outra ilegível aos que não tem acesso à essa chave. E a Matemática tem papel crucial nessa transformação. A palavra *criptografia* vem do grego e significa *escrita secreta* e segundo (COUTINHO, 2009), criptografia:

> "É a arte dos “códigos secretos”, que todos já praticamos quando criança".

Os números primos também têm um grande destaque nessa dissertação. Ao ensinarmos os números primos na educação básica, passamos ao aluno a falsa ideia de que esses números servem apenas para fazermos o mínimo múltiplo comum e o máximo divisor comum. Mas, ao estudarmos um pouco mais sobre esses incríveis números, percebemos o qual grandiosa é sua aplicação e suas particularidades. Unir o ensino dos números primos com a aplicação na criptografia se torna extremamente interessante e o aluno passa a enxergar a utilidade de seu aprendizado e esse passa a ter sentido.

Nossa dissertação tem por objetivo apresentar as Criptografias de chaves assimétricas *RSA* e *ElGamal* além dos conceitos matemáticos que as embasarão. Ela foi dividida em capítulos que se conectam e se complementam.

O primeiro capítulo trata-se deste texto introdutório com explicações do que será tratado ao longo desta monografia. No segundo capítulo nos dedicamos a falar sobre os *Números primos*, algumas definições e teoremas sobre sua importância e como todos os números naturais podem se originar deles. Apresentamos também algumas funções que geram os primos, embasados em estudos de matemáticos que se dedicaram para encontrar e formular tais funções. Em seguida, mostraremos como é a distribuição dos números primos, se a distância entre eles é infinita ou se há algum intervalo no qual sempre irá existir um número primo contido nele.

Apresentaremos alguns primos que são conhecidos como *Primos especiais*, primos que possuem alguma característica específica. E para saber se um determinado número grande é primo, estudaremos os *Testes de primalidade*.

Tudo que será explicado e mencionado no Capítulo 2 servirá de base para o Capítulo 3: Criptografias. Nesse capítulo serão apresentados os algoritmos de codificação e decodificação, exemplos práticos e suas respectivas autenticidades. Também apresentaremos o *Protocolo Diffie-Hellman*, um dos grandes avanços na área da criptografia, mais especificamente na troca de chaves.

Para aplicar o que foi exposto nessa dissertação, temos o Capítulo 4: Atividades. Sugerimos duas atividades para serem desenvolvidas pelos professores com os alunos dos anos finais do Ensino Fundamental ou Ensino Médio. Atividades que incentivam os alunos a praticar a Matemática de forma prazerosa e descontraída, mas sem deixar de lado suas propriedades.

Por fim, encerramos com as considerações finais deixando clara a importância de se aprender Matemática e mostrando suas contribuições para temas tão atuais.

Esta dissertação também possui dois apêndices, um sobre Congruências e outro sobre Logaritmo Discreto. Ambos apresentam teoremas e definições que servirão de base para o capítulo sobre os números primos e para o capítulo sobre criptografias.

2 NÚMEROS PRIMOS

Os números primos sempre foram e continuam sendo um dos grandes mistérios da Matemática. Sua infinidade e utilização ganham a atenção de muitos. A pergunta mais recorrente sobre esses números acabou sendo respondida por Euclides ao provar que existem infinitos números primos. Mas ainda restava descobrir uma expressão viável para encontrar todos os números primos ou, pelo menos, parte deles.

O fato é, os números primos nos auxiliam em várias questões matemáticas e sociais, como por exemplo a criptografia, tema central desta monografia.

Trataremos, nesse capítulo, de algumas definições e propriedades dos números primos que servirão como base para os próximos.

Definição 2.1 *Um número natural maior do que 1 é chamado número primo se possuir como divisores apenas o 1 e ele mesmo. Caso contrário, dizemos que o número é composto.*

Podemos dizer que, um número natural n é primo se, ao escrevermos n da forma $n = a.b$, com $a, b \in \mathbb{N}$, temos apenas duas opções: $a = 1$ e $b = n$ ou $a = n$ e $b = 1$. No caso do número natural $n = a.b$ ser composto, temos que $1 < a < n$ e $1 < b < n$.

Curiosidade: A palavra *primos* vem do latim *PRIMUS* que significa primeiro. Os números primos recebem esse nome por não serem formados por outros números, serem os "primeiros". Os outros números que podem ser formados pelo produto de números primos, são chamados de números *compostos*.

Notação: Usaremos a notação $a|b$ para dizer que a divide b quando existir $n \in \mathbb{Z}$ tal que $b = a.n$

Dados dois números primos p e q e um número inteiro qualquer a, temos que:

I) Se $p|q$, então $p = q$.

De fato, como $p|q$ e sendo q um número primo, temos que $p = 1$ ou $p = q$. Sendo p primo, temos que $p > 1$. Portanto, $p = q$.

II) Se $p \nmid a$, então $mdc(p,a) = 1$.

De fato, se $mdc(p,a) = d$, temos que $d|p$ e $d|a$. Logo, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$, consequentemente, $d = 1$.

Proposição 2.2 *Dois números inteiros a e b são primos entre si se, e somente se, existem inteiros m e n tais que* $ma + nb = 1$.

A demonstração da proposição anterior pode ser encontra em (HEFEZ, 2016).

Teorema 2.3 *Sejam* $a, b, c \in \mathbb{Z}$. *Se* $a|bc$ *e* $mdc(a,b) = 1$, *então* $a|c$.

Demonstração: Se $a|bc$, existe $y \in \mathbb{Z}$ tal que $bc = ay$. Se $mdc(a,b) = 1$, pela proposição anterior, temos que existem $m, n \in \mathbb{Z}$ tais que

$$ma + nb = 1.$$

Multiplicando ambos os membros da igualdade acima por c, temos:

$$mac + nbc = c.$$

Mas $bc = ay$, então

$$mac + nay = c$$

$$a.(mc + ny) = c.$$

Portanto, $a|c$.

■

Lema 2.4 *Sejam* $a, b, p \in \mathbb{Z}$, *com p primo. Se* $p|ab$, *então* $p|a$ *ou* $p|b$.

Demonstração: Suponhamos que $p|ab$ e, sem perda de generalidade, suponhamos que $p \nmid a$. Então, basta provar que $p \mid b$. Se $p \nmid a$, então $mdc(p,a) = 1$. Assim, pelo Teorema 2.3, $p|b$.

■

Corolário 2.5 *Se* $p, p_1, ..., p_n$ *são números primos e, se* $p|p_1...p_n$, *então* $p = p_i$ *para algum* $i = 1, .., n$.

A demonstração do corolário anterior pode ser encontrada em (HEFEZ, 2016).

Teorema 2.6 ***Teorema fundamental da Aritmética***

Todo número natural maior do que 1 *ou é primo ou se escreve de modo único como um produto de números primos.*

Demonstração: Para esta demonstração usaremos a segunda forma do Princípio da Indução Finita.

Se $n = 2$, o resultado é imediato. Suponhamos o resultado válido para todo número natural menor do que n e vamos mostrar que vale para n. Para n primo, não há o que demonstrar. Suponhamos então que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1.n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1...p_r$ e $n_2 = q_1...q_s$. Portanto $n = p_1...p_r.q_1...q_s$.

Agora, provaremos a unicidade da escrita. Suponhamos que tenhamos $n = p_1...p_r = q_1...q_s$, onde os p_i e os q_j são números primos. Como $p_1|q_1...q_s$, pelo Corolário 2.5, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, ..., q_s$ podemos supor que seja q_1. Portanto, $p_2...p_r = q_2...q_s$. Como $p_2...p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e os q_j são iguais aos pares.

■

Agrupando os fatores primos repetidos e ordenando os primos em ordem crescente no Teorema 2.6, temos o seguinte enunciado:

Teorema 2.7 *Dado um número inteiro $n \neq -1, 0, 1$, existem primos $p_1 < ... < p_r$ e $\alpha_1, ..., \alpha_r \in \mathbb{N}$ univocamente determinados, tais que*

$$n = \pm(p_1)^{\alpha_1}...(p_r)^{\alpha_r}.$$

O próximo teorema é considerado uma das grandes conquistas da Matemática. Mostraremos duas demonstrações do próximo teorema, uma de Euclides outra de Euler.

Teorema 2.8 *Existem infinitos números primos.*

Demonstração: Prova de Euclides Suponhamos, por absurdo, que exista apenas um número finito de números primos $p_1, ..., p_r$. Considere o número natural

$$n = p_1 p_2 ... p_r + 1.$$

Pelo Teorema 2.6, o número n é um número primo ou possui um fator primo p que, portanto deve ser um dos $p_1, ..., p_r$ e, consequentemente, divide o produto $p_1 p_2 ... p_r$. Mas isso implica que p divide 1, o que é absurdo. Portanto a sequência dos números primos é infinita.

■

Prova de Euler Suponhamos que a quantidade de números primos seja finita. São eles: $p_1, p_2, ..., p_m$. Considere $\tilde{P}$ definido pelo produto de m séries geométricas.

$$\tilde{P} = \left(\sum_{n=0}^{\infty} \frac{1}{p_1^n}\right) \cdot \left(\sum_{n=0}^{\infty} \frac{1}{p_2^n}\right) \cdots \left(\sum_{n=0}^{\infty} \frac{1}{p_m^n}\right).$$

As séries $\sum_{n=0}^{\infty} \frac{1}{P_j^n}$, com $1 \leq j \leq m$, são convergentes com soma

$$\sum_{n=0}^{\infty} \frac{1}{p_j^n} = \frac{1}{\left(1 - \frac{1}{p_j}\right)} = \frac{p_j}{p_j - 1}.$$

Portanto:

$$\tilde{P} = \left(\sum_{n=0}^{\infty} \frac{1}{p_1^n}\right) \cdot \left(\sum_{n=0}^{\infty} \frac{1}{p_2^n}\right) \cdots \left(\sum_{n=0}^{\infty} \frac{1}{p_m^n}\right) = \left(\frac{p_1}{p_1 - 1}\right)\left(\frac{p_2}{p_2 - 1}\right) ... \left(\frac{p_m}{p_m - 1}\right).$$

Pelo teorema fundamental da aritmética (Teorema 2.6) todo inteiro positivo é representado unicamente como $N = p_1^{n_1} \cdot p_2^{n_2} \cdots p_m^{n_m}$. Logo

$$\tilde{P} = \sum_{n_1,...,n_m=0}^{\infty} \frac{1}{p_1^{n_1} \cdot p_2^{n_2} \cdots p_m^{n_m}} = \sum_{N=1}^{\infty} \frac{1}{N} = \infty$$

Chegando assim a uma contradição. Portanto, o conjunto dos números primos é infinito.

■

2.0.1 Pequeno Teorema de Fermat

Segundo (HEFEZ, 2016), o teorema que iremos apresentar já era de conhecimento dos chineses há pelo menos 500 anos antes de Cristo, mas coube a Fermat, no século XVII, fazer sua generalização. Apesar de receber o nome de "pequeno" é de grande importância, dentre várias aplicações, para os testes de primalidade e para a criptografia. Antes de enunciarmos o Pequeno Teorema de Fermat, provaremo o seguinte lema:

Lema 2.9 *Seja p um número primo. Os números* $\begin{pmatrix} p \\ i \end{pmatrix} = p\frac{(p-1)...(p-i+1)}{i!}$, *com* $0 < i < p$, *são todos divisíveis por p.*

Demonstração: Para $i = 1$, o resultado segue de imediato. Suponhamos $0 < i < p$. Temos então que $i!|p.(p-1).(p-2)...(p-i+1)$. Mas como p é um número primo, temos que $mdc(i!, p) = 1$. Assim, $i!|(p-1).(p-2)...(p-i+1)$. Provando assim que p divide $\begin{pmatrix} p \\ i \end{pmatrix}$.

■

Teorema 2.10 (Pequeno Teorema de Fermat) *Dado um número primo p, tem-se que p divide o número* $a^p - a$, *para todo* $a \in \mathbb{Z}$.

Demonstração: Se $p = 2$, o resultado é óbvio já que $a^2 - a = a(a-1)$ é par. Suponhamos p ímpar. Nesse caso, basta mostrar o resultado para $a \geq 0$. Para $a = 0$, o resultado vale pois $p|0$. Suponhamos o resultado válido para a, iremos prová-lo para $a+1$. Pela fórmula do Binômio de Newton,

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

Pelo Lema 2.9 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, o resultado segue.

■

Uma outra forma de enunciar o *Pequeno Teorema de Fermat* usando a notação de congruência é:

Se p é um número primo e $a \in \mathbb{Z}$, então

$$a^p \equiv a \ \ mod p.$$

Mais ainda, se $p \nmid a$, então

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

2.1 FUNÇÕES QUE GERAM OS PRIMOS

Quando pensamos em números naturais, conseguimos facilmente separá-los em pares e ímpares. Se um número for da forma $n = 2.m$, com n e m naturais, ele será par; mas se for da forma $n = 2.m + 1$, então será ímpar. Sendo assim, conseguimos uma fórmula para indicar quando um número é par e quando ele é ímpar.

Será que com os números primos e compostos também conseguimos uma fórmula, uma função para sabermos quando é um e quando é outro?

Podemos pensar em três tipos de funções, ou fórmulas, para determinar se um número é primo ou composto. São elas:

i) $f(n) = p_n$, n inteiro para todo $n \geq 1$;

ii) $f(n)$ é sempre um número primo e se $n \neq m$ então $f(n) \neq f(m)$;

iii) o conjunto de números primos é igual ao conjunto de valores positivos assumido pela função.

Percebemos facilmente que a primeira condição é a mais ampla e a que mais nos chama a atenção. Ela quer encontrar *todos* os primos *em ordem*. Já a segunda condição quer encontrar um infinidade de primos, mas não são todos e nem necessariamente em ordem. Por fim, a terceira condição quer encontrar uma função que descreva o conjunto dos números primos.

Exemplo 2.11 *Um exemplo, não muito útil, da condição (i) é:*

$$P_N = 1 + \sum_{M=1}^{2^N} \left\lfloor \sqrt[N]{\frac{N}{1+\pi(M)}} \right\rfloor,$$

sendo $\lfloor X \rfloor$ a parte inteira de X e $\pi(M)$ a quantidade de números primos menores do que ou iguais ao x.

Obtida por Willians (1964) é uma fórmula muito extensa e acaba se tornando inútil. Para termos uma ideia, se queremos encontrarmos o décimo primo, devemos contar quantos primos existem até 1024:

$$P_{10} = 1 + \sum_{M=1}^{1024} \left\lfloor \sqrt[10]{\frac{N}{1+\pi(M)}} \right\rfloor = 29.$$

Exemplo 2.12 *Um exemplo da condição (ii) pode ser dado por:*

$$f(N) = \left\lfloor 2^{2^{2^{\cdots^{w}}}} \right\rfloor,$$

sendo $\lfloor X \rfloor$ *a parte inteira de* X.

$\left\lfloor 2^{2^{2^{\cdots^{w}}}} \right\rfloor$ *representa N etapas de expoentes e* $w = 1,92827800\ldots$.

Obtida por Wright (1954), essa fórmula usa uma aproximação para w, o que gera erros e acabamos obtendo números que não são primos. Tornando-a assim pouco útil.

Com relação à condição (iii), como iremos ver, não existe uma função polinomial com uma única variável que gere todos os números primos, nem um algoritmo polinomial eficiente que encontre os fatores de qualquer número natural composto. O que temos são algumas conjecturas e fórmulas que encontram uma parte dos primos. Veremos algumas delas com mais detalhes nas seções seguintes.

Teorema 2.13 *Se* $f(X)$ *é um polinômio não-constante, com coeficientes inteiros e uma variável, existem infinitos inteiros n tais que* $|f(n)|$ *não é primo.*

Demonstração: Suponhamos que exista algum inteiro $n_0 \geq 0$ tal que $|f(n_0)| = p$ primo. Sabendo que o polinômio não é constante, temos que

$$\lim_{n\to\infty} |f(n)| = \infty.$$

Então, existe $n_1 > n_0$ tal que, se $n \geq n_1$, então $|f(n)| > p$. Assim, para todo inteiro h tal que $n_0 + ph \geq n_1$, tem-se que $f(n_0 + ph) = f(n_0) +$ (múltiplo de p) = (múltiplo de p). Como $|f(n_0 + ph)| > p$, temos que $|f(n_0 + ph)|$ é um número composto.

■

Pelo teorema anterior, vimos que um polinômio com coeficientes inteiros e uma única variável não fornece apenas números primos.

2.1.1 O polinômio de Euler

Veremos nesta seção um dos mais famosos polinômios geradores de primos, o *Polinômio de Euler*, descoberto por Euler em 1772. O *Polinômio de Euler* dado pela função polinomial

$$P(n) = n^2 - n + 41,$$

é um ótimo exemplo de função capaz de gerar uma grande sequência de números primos. Ao analisarmos a função, conseguimos perceber facilmente que, se n for um múltiplo de 41, então o número gerado não será primo, pois será múltiplo de 41 devido a sua forma.

Para $n = 0, 1, 2, 3, ..., 39$, todos seus valores são números primos. São eles, respectivamente: 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523 e 1601.

Curiosidade: Nesse polinômio de Euler, se tomarmos o polinômio $P(n) = n^2 + n + 41$, que se diferencia do $P(n)$ apenas na mudança de sinal da variável de primeiro grau, com os valores de n = 1, 2, 3, ..., 40 os primos encontrados são os mesmos.

2.1.2 Outros polinômios

Existem outros polinômios quadráticos que também produzem uma grande quantidade de números primos. Veja em (RIBENBOIM, 2004). Alguns exemplos:

i) **Polinômio de Legendre**

Legendre observou que os polinômios da forma $2x^2 + q$, com $q = 3, 5, 11$ *e* 29 possuem a maior quantidade de primos possíveis. Para outros valores de q a quantidade de número primos encontrada é menor.

ii) **Polinômio de A. Lévy**

A. Lévy (1914) observou que $3x^2 + 3x + 23$ produz 22 primos.

iii) **Polinômio de Pol e Speziali**

Pol e Speziali (1951), encontraram 29 primos com o polinômio $6x^2 + 6x + 31$.

iv) **Polinômio de R. Ruby**

O polinômio quadrático $f(x) = 36x^2 - 810x + 2753$, descoberto por R. Ruby (1990), é atualmente o polinômio de uma variável que produz a maior quantidade de primos com sucessivos valores iniciais tais que $|f(k)|$ é primo, com $k = 0, 1, 2..., 44$.

v) **Polinômio de Dress e Landreau**

Dress e Landreau (2003) descobriram polinômios de grau superior, são eles:

$$f(x) = 66x^3 + 83x^2 - 13735x + 30139$$

sendo $|f(x)|$ primo quando $-26 < x < 19$, obtendo 46 números primos; e

$$f(x) = 16x^4 + 28x3 - 1685x^2 - 2380x + 110647,$$

que gera 46 números primos para $|f(x)|$ quando $-2 < x < 22$.

2.1.3 Polinômio gerador de todos os números primos

Na seção anterior, vimos que todos os polinômios com uma única variável geram apenas uma parte dos números primos. Surgem então a seguinte questão: e se o polinômio tiver mais de um variável?

Existe sim um polinômio que gere todos os números primos! Um polinômio com coeficientes inteiros, sendo que o conjunto de números primos coincide com o conjunto dos números naturais assumidos por esse polinômio. O único detalhe é que um número primo pode aparecer mais de uma vez.

Matijasevc (1971) descobriu um polinômio com grau 37 e 24 variáveis. Posteriormente, ao fazer a tradução de sua descoberta para o inglês, esse polinômio foi aprimorado e contém 21 variáveis e grau 21.

Jones, Sato, Wada e Wiens (1976), descobriram um polinômio com grau 25 e 26 variáveis que encontram todos os número primos. É ele:

$$\begin{gathered}
(k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2 \\
-[2n+p+q+z-e]^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 \\
-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2 \\
-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2 \\
+1-(x+cu)^2]^2-[n+l+v-y]^2-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2 \\
-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2 \\
-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 \\
-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}.
\end{gathered}$$

A demonstração pode ser encontrada em (RIBENBOIM, 2004).

Além desse polinômio que acabamos de ver, segundo Honsberger (1976) existe uma função que gera os número primos. Antes de vermos tal função iremos enunciar o Teorema de Wilson que será utilizado em sua demostração.

Teorema 2.14 ***Teorema de Wilson:*** *Um número p é primo se, e somente se*

$$(p-1)! \equiv -1 \quad mod\ p.$$

O *Teorema de Wilson* será demonstrado na seção de *Testes de primalidade*.

Proposição 2.15 *Sejam x e y números naturais com* $y \neq 0$ *e* $a = x(y+1) - (y!+1)$*, então*

$$f(x,y) = \frac{y-1}{2}\left[|a^2-1| - (a^2-1)\right] + 2$$

nos dá todos os números primos e somente estes.

Demonstração: Primeiro mostraremos que a função $f(x,y)$ sempre será um número primo e em seguida que ela fornece todos os números primos.

Note que a admite valores inteiros já que x e y são naturais, assim temos dois casos: $a^2 \geq 1$ e $a^2 = 0$.

i) Se $a^2 \geq 1$ temos que $a^2 - 1 \geq 0$, então $|a^2-1| = a^2-1$. Logo, $f(x,y) = 2$, que é um número primo.

ii) Se $a^2 = 0$, temos:

$$f(x,y) = \frac{y-1}{2}\left[|-1| - (-1)\right] + 2 = y+1.$$

Como $a^2 = 0$, então $x(y+1) - (y!+1) = 0$, ou seja, $x(y+1) = (y!+1)$. Assim, $(y+1)|(y!+1)$. Fazendo $y = p-1$ temos o Teorema de Wilson:

$$p|(p-1)!+1.$$

Logo $y+1$ é um número primo. Concluímos então que, para quaisquer valores naturais de x e y a função $f(x,y)$ será um número primo.

Como $f(x,y)$ é primo para $a = 0$, temos $x(y+1) - (y!+1) = 0$. Assim, temos que

$$x = \frac{y!+1}{y+1}$$

e, tomando $y = p-1$, com p primo, teremos

$$x = \frac{(p-1)!+1}{p},$$

o que nos dá

$$f\left(\frac{(p-1)!+1}{p}, p-1\right) = p.$$

Portanto $f(x,y)$ fornece todos os números primos.

■

2.2 DISTRIBUIÇÃO DE NÚMEROS PRIMOS

Já sabemos que existem infinitos números primos. Porém, não sabemos nada relativo a sua distribuição dentro dos números naturais. Será que existe um intervalo no qual os números primos estão mais concentrados? O objetivo desta seção é apresentar alguns resultados que mostram como os números primos se distribuem e alguns resultados clássicos.

Usaremos como referência para esta seção (RIBENBOIM, 2004) e (COUTINHO, 2016).

Sabemos que qualquer inteiro na divisão por 6 deixa resto 0, 1, 2, 3, 4 ou 5. Como queremos encontrar os números primos, os restos 0, 2 e 4 não nos convém pois tornariam o número divisível por 2; o resto 3, tornaria o número divisível por 3. Portanto, se p for primo só pode deixar resto 1 ou resto 5 quando dividido por 6. Isso nos leva a conjecturar que existem infinitos primos da forma $6N+5$.

Teorema 2.16 *Existem infinitos números primos da forma* $6N+5$.

Demonstração: Suponhamos que

$$\mathbb{P} = \{5, p_1, ..., p_s\},$$

seja um conjunto finito formado apenas por números primos da forma $6N+5$. Considere os números

$$N = p_1.p_2 \cdots p_s \quad e \quad 6N+5.$$

Pelo teorema da fatoração única, podemos escrever $6N+5$ na forma

$$6N+5 = q_1^{\alpha_1} \cdots q_m^{\alpha_m},$$

em que os q_i são primos positivos e α_i são inteiros positivos. Como $6N+5$ é ímpar, todos os seus fatores têm que ser ímpares. Assim, os q_i são ímpares e deixam resto 1 ou 5 na divisão por 6. Suponhamos que todos os q_i deixem resto 1 na divisão por 6. Desta forma, teríamos que

$$q_1^{\alpha_1} \cdots q_m^{\alpha_m} \equiv 1 \; mod \; 6.$$

Mas isso é impossível, pois

$$q_1^{\alpha_1} \cdots q_m^{\alpha_m} \equiv 6N+5 \equiv 5 \; mod \; 6$$

e 1 e 5 não são congruentes módulo 6.

O que nos leva a concluir que $6N+5$ tem pelo menos um fator primo que deixa resto 5 quando dividido por 6.

Como $\mathbb{P}$, por hipótese, é o conjunto com todos os primos da forma $6N+5$, então $6N+5$ é divisível por algum elemento de $\mathbb{P}$.

Primeiramente, temos que 5 não divide $6N+5$, pois se dividisse, teria que dividir também

$$6N = (6N+5) - 5 = 6N = 2 \cdot 3 \cdot p_1 \cdots p_s$$

o que não acontece pelo fato de 5 não estar entre os primos dessa fatoração.

Por outro lado, se $6N+5$ fosse divisível por um dos primos que divide N, então $(6N+5) - 6N = 5$, seria divisível pelo mesmo primo, o que também não é possível.

Mostrando assim que $6N+5$ não pode ser divisível por nenhum elemento de $\mathbb{P}$, o que nos leva a contradição.

Portanto, há uma quantidade infinita de primos da forma $6n+5$.

■

O que acabamos de provar foi um caso particular do **Teorema de Dirichlet** enunciado a seguir

Teorema 2.17 *Dados inteiros a e b primos entre si, então existe infinitos primos da forma* $an+b$*, com n natural.*

Outro resultado clássico é o **Postulado de Bertrand** (1845): Seja n um inteiro positivo. Então sempre existe um primo p tal que $n \leq p \leq 2n$.

As demonstrações do Teorema de Dirichlet e o Postulado de Bertrand podem ser encontradas em (MARTINEZ; SALDANHA; TENGAN, 2011).

Esse postulado foi verificado por ele mesmo para todos os números até $2,3 \cdot 10^6$.

2.2.1 Teorema dos números primos

Antes de prosseguir, definiremos $\pi(x)$ como sendo a quantidade de números primos tais que $2 \leq p \leq x$.

Apresentaremos agora algumas descobertas sobre a função $\pi(x)$ em ordem cronológica. Veja em (RIBENBOIM, 2004).

Euler

Como visto anteriormente, Euler demostrou que a soma dos inversos dos primos é divergente, provando a infinidade deles. Euler também observou que para todo número real $\sigma > 1$ a série

$$\sum_{n=1}^{\infty} \left(\frac{1}{n^{\sigma}} \right)$$

é convergente. Definindo assim, uma função $\zeta(\sigma)$, conhecida como *função zeta*. A função zeta expressa a fatoração de números inteiros como produto de números primos:

$$\zeta(\sigma) = \prod_{p} \frac{1}{1 - \frac{1}{p^{\sigma}}} \quad , para\ \sigma > 1.$$

Legendre

Legendre (1808), utilizando o Crivo de Erastóstenes, provou que:

$$\pi(N) = \pi\sqrt{N} - 1 + \sum \mu(d) \left\lfloor \frac{N}{d} \right\rfloor,$$

o somatório é sobre todos os divisores d do produto de todos os primos $p \leq \sqrt{N}$ e sendo

$\mu(d)$ a função de *Möbius* definida por:

$$\begin{cases} \mu(1) = 1; \\ \mu(n) = (-1)^r, \textit{ se n for o produto de r primos distintos}; \\ \mu(n) = 0, \textit{ se o quadrado de um número primo divide n}. \end{cases}$$

Como consequência desse resultado, Legendre mostrou que:

$$\lim_{n\to\infty}\left(\frac{\pi(x)}{x}\right) = 0.$$

Gauss

Com apenas 15 anos de idade, Gauss (1792) conjecturou que $\pi(x)$ era assintoticamente igual à função:

$$Li(x) = \int_2^x \frac{dt}{log\, t}.$$

Tschebycheff

Tschebycheff (1850) obteve grande avanço em determinar a magnitude de $\pi(x)$ e mostrou que

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

se o limite existir.

Riemann

Riemann, ao tentar obter uma melhor aproximação para $\pi(x)$, começou a estudar a função zeta e a estendeu para números complexos com partes reais maiores do que 1. A aproximação para a $\pi(x)$ obtida por Riemann ficou conhecida como *Função de Riemann*:

$$R(x) = \sum_{n=1}^{\infty}\frac{\mu(n)}{n}Li(x^{1/n}),$$

Foi Riemann quem forneceu várias ferramentas para que se conseguisse provar o *Teorema dos Números Primos*:

Teorema 2.18 ***(Teorema dos números primos)*** *Seja $\pi(x)$ a quantidade de números primos tais que $2 \leq p \leq x$. Temos que*

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

A demonstração desse teorema pode ser encontrada em (MARTINEZ; SALDANHA; TENGAN, 2011)

2.2.2 Novo teorema sobre a distribuição dos números primos

Tivemos, recentemente, grandes avanços em relação à distância entre dois números primos. Os maiores responsáveis por esses avanços foram: Yitang Zhang e James Maynard.

Yitang Zhang

Yitang Zhang, nasceu em Xangai, China e desde muito novo já dava sinais de suas habilidades com a Matemática. Mesmo tendo sido forçado a parar de frenquentar uma escola, devido a Revolução Cultural antiintelectual, Zhang nunca parou seus estudos e aos 23 anos ingressou na Universidade de Pequim, fez mestrado e aos 29 anos fez seu doutorado na Purdue University em Lafayette, Indiana. Após seu doutorado, Zhang trabalhou por cerca de sete anos com empregos temporários. Apenas aos 44 anos, Zhang conseguiu um emprego como professor de Matemática e dez anos depois, em 2009, começou estudar mais de perto a conjectura dos primos gêmeos. O trabalho de Zhang foi tentar provar que os números primos não ficam infinitamente distantes uns dos outros. Em 2013, Zhang mostrou que existem infinitos pares de primos que estão a menos de 70 milhões de unidades uns dos outros. Zhang acredita que consegue reduzir esse valor. Veja em (LIN, 2015)

O método utilizado por ele tem base no trabalho de Goldston, Pintz e Yıldırım sobre as lacunas entre primos consecutivos e o teorema de Bombieri-Vinogradov.

Teorema 2.19 *Seja* $\mathrm{H} = \{h_1, h_2, ..., h_{k_0}\}$ *um conjunto admissível de inteiros não negativos com* $k_0 \geq 3,5 \times 10^6$. *Existem infinitos inteiros positivos n tais que a* k_0*-tupla*

$$\{n+h_1, n+h_2, ..., n+h_{k_0}\}$$

contém pelo menos dois primos. Consequentemente, temos:

$$\liminf_{n\to\infty}(p_{n+1} - p_n) < 7 \times 10^7.$$

A demonstração desse teorema pode ser encontrado em (ZHANG, 2014)

James Maynard James Maynard, de apenas 26 anos, começava seus estudos sobre as lacunas entre os números primos ao mesmo tempo que Yitang Zhang apresentava sua descoberta. Maynard deu sequência em seus estudos e poucos meses depois de Zhang conseguiu provar, com uma abordagem completamente independente, que existem infinitos pares de primos a uma distância menor do que 600 unidades. Maynard ainda foi além, sua abordagem se aplicava para triplos, quádruplos e outras coleções maiores, mudando apenas o limite de cada uma. Veja (KLARREICH, 2020).

Teorema 2.20 *Seja p_i o i-ésimo número primo, temos que*

$$\liminf_n (p_{n+1} - p_n) < 600.$$

Para a demonstração desse teorema, Maynard utiliza apenas o teorema de Bombieri-Vinogradov. Ver (MAYNARD, 2019).

2.3 PRIMOS ESPECIAIS

Mostraremos, nesta seção, alguns números primos especiais. São eles: primos de Fermat, Mersenne, Sophie Germain e primos gêmeos.

Para as demonstrações de alguns resultados desses números primos devemos relembrar algumas proposições sobre divisibilidade.

Proposição 2.21 *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a-b$ divide $a^n - b^n$.*

Demonstração: A prova será feita por indução sobre n.

Para $n = 1$, a afirmação é verdadeira, pois $a-b$ divide $a^1 - b^1 = a - b$.

Suponhamos que $a-b|a^n - b^n$. Assim,

$$a^{n+1} - b^{n+1} = a.a^n - b.b^n = a.a^n - b.a^n + b.a^n - b.b^n = (a-b).a^n + (a^n - b^n).b$$

Como $a-b|a-b$ e, por hipótese, $a-b|a^n - b^n$, temos que:

$$a-b|(a-b).a^n \text{ e } a-b|(a^n - b^n).b$$

Assim, $a-b|a^{n+1} - b^{n+1}$. Portanto, o resultado é valido para todo $n \in \mathbb{N}$.

■

Proposição 2.22 *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a+b$ divide $a^{2n+1} + b^{2n+1}$.*

Demonstração: Esta demonstração também será feita por indução em n.

Claramente, temos que a afirmação é válida para $n = 0$, pois $a+b$ divide $a^1 + b^1 = a+b$. Suponhamos que $a+b | a^{2n+1} + b^{2n+1}$. Assim

$$\begin{aligned} a^{2(n+1)+1} + b^{2(n+1)+1} &= a^2 a^{2n+1} - b^2 a^{2n+1} + b^2 a^{2n+1} + b^2 b^{2n+1} \\ &= (a^2 - b^2) a^{2n+1} + b^2 (a^{2n+1} + b^{2n+1}). \end{aligned}$$

Como $a+b$ divide $a^2 - b^2 = (a+b).(a-b)$ e , por hipótese, $a+b | a^{2n+1} + b^{2n+1}$, temos que

$$a+b | a^{2(n+1)+1} + b^{2(n+1)+1}.$$

Portanto, o resultado é válido para todo $n \in \mathbb{N} \cup 0$.

■

2.3.1 Primos de Fermat

Pierre de Fermat nasceu em 1601, na França, e morreu em 1665. Foi advogado e oficial do governo em Toulouse. Apesar de não ter a Matemática como sua principal atividade e não ter tido interesse em publicar suas descobertas, Fermat é lembrado por seu legado incrível. Uma de suas contribuições, da qual falaremos agora, ficou conhecida como *Números de Fermat*.

Vejamos a seguinte proposição:

Proposição 2.23 *Sejam a e n números naturais maiores do que 1. Se $a^n + 1$ é primo, então a é par e $n = 2^m$, com $m \in \mathbb{N}$.*

Demonstração: Suponhamos que $a^n + 1$ seja primo, com $a, n > 1$. Assim, temos que a é par, pois caso contrário, $a^n + 1$ seria par maior que 2 contrariando o fato de ser primo. Se n tivesse um divisor primo p diferente de 2, teríamos $n = n_1 p$ com $n_1 \in \mathbb{N}$. Pela Proposição 2.22, $a^{n_1} + 1$ dividiria $(a^{n_1})^p + 1 = a^n + 1$. Mas isso contraria o fato de $a^n + 1$ ser primo. Implicando assim que n é da forma 2^m.

■

Os números conhecidos como *números de Fermat* são da forma

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, ...$$

Os números de Fermat que são primos receberam o nome de *Primos de Fermat*.

Curiosidade: O maior número de Fermat para o qual se conhece um fator é $F(23471)$: $2^{2^{23471}} + 1$; o fator é $5.2^{23473} + 1$. Esse também é o maior número de Fermat composto que se sabe.

Outra grande contribuição de Fermat, denominada *Último Teorema de Fermat*, será vista na próxima seção com os *primos de Sophie German*.

2.3.2 Primos de Sophie Germain

Sophie Germain, nasceu em Paris, França, no ano de 1776. Quando tinha 13 anos de idade, teve início a Revolução Francesa, o que tornou necessário sua permanência em casa e assim desencadeou seu interesse pelos estudos. Seu interesse pela Matemática surgiu após ler sobre a história do assassinato de Arquimedes por um soldado. O assassinato ocorreu pelo fato de Arquimedes estar mais preocupado com seus estudos em Geometria do que com o ataque.

Mas, como podemos imaginar, não foi fácil para Sophie German, uma mulher, estudar assuntos científicos mais aprofundados naquela época. Inicialmente, seus pais a proibiram de estudar e as instituições não aceitavam mulheres. Sophie persistiu e obteve aceitação dos pais e usou um pseudônimo masculino em seus trabalhos e comunicações com outros matemáticos.

Para conhecer mais sobre Sophie German, veja (WIKIPéDIA, 2020c).

Sophie Germain mostrou um caso particular do último teorema de Fermat que afirmava:

$$x^n + y^n = z^n \text{ , era válido apenas para } n = 2,$$

sendo $x, y, z \in \mathbb{Z}$ e $n \in \mathbb{N}$.

Sophie Germain provou que a afirmação de Fermat estava correta para $n = p$, quando p e $2p + 1$ são números primos. Devido à essa prova, os números primos p tais que $2p + 1$ também são primos, são conhecidos como *primos de Sophie Germain*. Como exemplos temos o 3 e 7, 5 e 11 e vários outros.

Proposição 2.24 *Se p e $2p + 1$ são primos com $p > 2$, então não existem inteiros x, y, z com $mdc(x, y, z) = 1$ e $p \nmid xyz$ tais que $x^p + y^p + z^p = 0$.*

Demonstração: Demonstraremos esse resultado por contradição. Suponha que existam x, y, e z com $mdc(x,y,z) = 1$ e $p \nmid xyz$ tais que $x^p + y^p + z^p = 0$.

Afirmação 1: $2p+1|xyz$, caso contrário o pequeno teorema de Fermat implicaria que $x^{2p} \equiv 1 \ \ mod(2p+1)$. Logo $x^{2p} - 1 \equiv 0 \ \ mod(2p+1)$. O que equivale a $(x^p - 1)(x^p + 1) \equiv 0 \ mod(2p+1)$. Como $2p+1$ é primo, temos que $x^p \equiv 1 \ mod(2p+1)$ ou $x^p \equiv -1 \ mod(2p+1)$, isto é, $x^p \equiv \pm 1 \ \ mod(2p+1)$. Com raciocínio análogo ao caso anterior, concluímos que $y^p \equiv \pm 1 \ \ mod(2p+1)$ e $z^p \equiv \pm 1 \ \ mod(2p+1)$. Independente de qual caso ocorra, temos que

$$x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 \ \ mod(2p+1),$$

o que é um absurdo. Portanto,$2p+1|xyz$.

Do fato de $p > 2$ ser primo e $x^p + y^p + z^p = 0$, temos

$$(-x)^p = y^p + z^p$$

$$(-x)^p = (y+z).(y^{p-1} - y^{p-2}z + ... - yz^{p-2} + z^{p-1}).$$

Afirmação 2: os fatores do lado direito da igualdade $(y+z)$ e $(y^{p-1} - y^{p-2}z + ... - yz^{p-2} + z^{p-1})$ são primos entre si.

Suponha que q seja um primo que divide ambos os termos então $q|x$ e

$$y + z \equiv 0 \ \ mod \ q$$

$$y \equiv -z \ \ mod \ q \tag{2.1}$$

e

$$y^{p-1} - y^{p-2}z + ... - yz^{p-2} + z^{p-1} \equiv 0 \ \ mod \ q$$

usando a congruência 2.1, temos que

$$y^{p-1} - y^{p-2}z + ... - yz^{p-2} + z^{p-1} \equiv py^{p-1} \ \ mod \ q.$$

Como $q|x$ e $p \nmid xyz$ então $p \neq q$. Dos fatos que $q|x$, $q|py^{p-1}$ e $p \neq q$, segue que $q|y$.

Se isso ocorrer $z \equiv -y \equiv 0 \ \ mod \ q$. Desse modo, $q|x$, $q|y$ e $q|z$, um absurdo. Pois $mdc(x,y,z) = 1$.

Assim, pelo teorema da fatoração única em primos, existem inteiros a e d tais que

$$a^p = y + z \tag{2.2}$$

$$d^p = y^{p-1} - y^{p-2}z + \ldots - yz^{p-2} + z^{p-1} \tag{2.3}$$

Aplicando o raciocínio anterior para $(-y)^p = x^p + z^p$ e $(-z)^p = x^p + y^p$, concluímos que existem inteiros b, c, e e f, tais que

$$b^p = x + z \tag{2.4}$$

$$e^p = x^{p-1} - x^{p-2}z + \ldots - xz^{p-2} + z^{p-1} \tag{2.5}$$

$$c^p = x + y \tag{2.6}$$

$$f^p = x^{p-1} - x^{p-2}y + \ldots - xy^{p-2} + y^{p-1} \tag{2.7}$$

Como $2p+1|xyz$, podemos supor, sem perda de generalidade, que $2p+1|x$. Somando as equações 2.4 e 2.6 obtemos

$$b^p + c^p = 2x + y + z$$

$$2x = b^p + c^p - (z + y)$$

Utilizando a equação 2.2, concluímos que

$$2x = b^p + c^p - a^p$$

Do fato que $p > 2$, $2p+1$ é primo e $2p+1|x$, temos que $2p+1|b^p + c^p - a^p$.

Utilizando a afirmação 2 e os argumentos da demonstração da afirmação 1, concluímos que $2p+1|abc$.

Para terminar a demonstração dividiremo-na em dois casos.

Caso 1:

$2p+1|b^p = x+z$ ou $2p+1|c^p = x+y$. Do fato que $2p+1|x$ e $2p+1|x^p+y^p+z^p = 0$, obtemos que $2p+1|mdc(x,y,z) = 1$, o que é um absurdo.

Caso 2:

$2p+1|a^p$ Como $2p+1|x$ e $f^p = x^{p-1} - x^{p-2}y + ... - xy^{p-2} + y^{p-1}$, temos que $f^p \equiv y^{p-1} \ mod(2p+1)$.

Sabemos que $2p+1|a^p$ e $2p+1$ é primo. Logo, $2p+1|a$. Desse último fato e da afirmação 2, concluímos que $2p+1 \nmid d$.

Já que $2p+1|a$ e $a^p = y+z$ obtemos

$$y \equiv -z \ mod(2p+1) \tag{2.8}$$

Da congruência 2.8 e da equação 2.3, concluímos

$$d^p \equiv py^{p-1} \ mod(2p+1).$$

Assim, $2p+1|f$, caso contrário, teríamos

$$\pm p \equiv pf^p \equiv py^{p-1} \equiv d^p \equiv \pm 1 \ mod(2p+1),$$

o que é um absurdo.

Como $2p+1|f$ e $2p+1|x$, da equação 2.7, concluímos que $2p+1|y$. Como $y \equiv -z \ mod(2p+1)$ segue que $2p+1|z$. Novamente $2p+1|x$, $2p+1|y$ e $2p+1|z$, o que é impossível já que $mdc(x,y,z) = 1$.

■

Curiosidade: o teorema de Fermat surgiu a partir do estudo do teorema de Pitágoras. Fermat queria saber se para outras potências o teorema também estava correto. Infelizmente, Fermat faleceu achando que o teorema era válido apenas para $n = 2$. Veja mais em (WIKIPÉDIA, 2020b).

2.3.3 Primos de Mersenne

Marin Mersenne nasceu em uma família da classe trabalhadora, em 8 de setembro de 1588, na França. Aos dezesseis anos, Mersenne foi estudar na recém-criada Escola Jesuíta em

La Flèche, que havia sido criada como uma escola modelo para beneficiar todas as crianças, independentemente da condição financeira de seus pais. Ao contrário do desejo de seu pai, que queira que Mersenne seguisse carreira na igreja, ele foi para Paris dar sequência em seus estudos.

"Mersenne estava começando a perceber que, ao lado da religião, era a ciência que realmente o interessava. Matemática foi a área que estudou com maior profundidade, acreditando que sem ela nenhuma ciência seria possível. Ele sempre teve uma abordagem filosófica da matemática e acreditava que a causa das ciências é a causa de Deus". Veja (O'CONNOR,J.J. AND ROBERTSON, E.F., 1996).

Curiosidade: Dentre seus muitos interesses, a música foi um deles. Passou um bom tempo estudando sobre a velocidade e a acústica do som. Mersenne (1627) publicou uma obra na qual falava das leis relativas à corda vibrante, dizendo que sua frequência é proporcional à raiz quadrada da tensão e inversamente proporcional ao comprimento, ao diâmetro e à raiz quadrada do peso específico da string, de forma que quando uma dessas condições for alterada, todas as outras permaneçam as mesmas.

Mersenne é muito lembrado pelos famosos *Números de Mersenne*, aqueles que têm a forma $2^n - 1$, para algum inteiro n. Sendo que os maiores primos conhecidos que se tenha relato são todos da forma: $M_n = 2^n - 1$, para $n = 43112609, 42643801, 37156667, 32582657, 30402457, 25964951, 24036583, 20996011, 134669717$.

Inicialmente, acreditava-se que para todo p primo, os números de Mersenne fossem primos. No entanto vários matemáticos como Hudalricus Regius (1536), Pietro Cataldi (1603), Fermat (1640), Euler (1738), Lucas (1876) refutaram essa informação. Apenas em 1947 foi feita uma lista com os números até 257 que tornam os números de Mersenne primos, são eles:

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \; e \; 127.$$

Desde 1951, são usados computadores para procurarem números primos grandes e os valores de n para os quais M_n é primo são:

521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 232009, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011,24036583, 25964951, 30402457, 32582657, 37156667, 42643801 e 43112609.

Curiosidade: Os últimos dez números foram encontrados com a ajuda de computadores pessoais. Hoje ainda é possível participar dessa busca através do site: www.mersenne.org .

Vimos que nem todos os números de Mersenne, $M_n = 2^n - 1$, são primos. Agora, veremos que os números de Mersenne só tem chance de serem primos quando n é primo.

Proposição 2.25 *Sejam a e n números naturais maiores do que 1. Se $a^n - 1$ é primo, então $a = 2$ e n é primo.*

Demonstração: Admitiremos que $a^n - 1$ é um número primo, com $a, n > 1$.

Suponhamos, por absurdo, que $a > 2$. Assim, a Proposição 2.21 implica que $a - 1 > 1$ e $(a-1)|(a^n - 1)$. Absurdo, pois contraria o fato de $a^n - 1$ ser primo.

De forma análoga, podemos supor, por absurdo, que n não é primo. Temos que $n = rs$ com $r, s > 1$. Como $2^r - 1$ divide $(2^r)^s - 1 = 2^n - 1$, novamente, a Proposição 2.21 implica que $a^n - 1$ não é primo, absurdo. Logo, n é primo.

■

Dado um número natural n qualquer é difícil determinar se n é primo ou não. Já para os números de Mersenne, temos métodos muito eficazes para dizer se esse número é primo ou não. Por esse motivo, o maior número primo conhecido sempre é um de primo de Mersenne. Na seção *Teste de Primalidade* apresentaremos um algoritmo que fatora primos de Mersenne em tempo polinomial.

2.3.4 Primos gêmeos

Definição 2.26 *Dois números primos p e q, com $p > q$, são chamados de números primos gêmeos se $p = q + 2$.*

Em outras palavras, o par de números primos da forma p e $p+2$, são chamados primos gêmeos.

Alguns exemplos de *primos gêmeos* são 3 e 5, 11 e 13, 149 e 151, 191 e 193, 239 e 241. Mas a medida que os números aumentam fica mais difícil identificá-los. O maior par de números gêmeos conhecido até o momento é:

$$2.003.663.613 \times 2^{195.00} - 1, 2.003.663.613 \times 2^{195.00} + 1.$$

Assim como havia a grande curiosidade de saber se existiam infinitos números primos, também há a curiosidade de saber se os primos gêmeos são infinitos. Será que existem infinitos pares de números da forma $(p, p+2)$?

Essa pergunta é uma famosa conjectura dos números primos gêmeos e será trabalhada na seção *Problemas em aberto*.

Teorema 2.27 *Sejam p e p+2 primos gêmeos. Então,*

$$\sum_{p,p+2primos} \frac{1}{p} < \infty$$

Brun mostrou que $\sum_{p,p+2primos} \frac{1}{p} < \infty$ converge para 1,9021605824283 , chamada constante de Brun.

$$B = \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{7}+\frac{1}{9}\right)+...+\left(\frac{1}{p}+\frac{1}{p+2}\right) = 1,9021605824283.$$

Devido ao fato da soma de seus inversos ser convergente, acredita-se que há um quantidade finita de primos gêmeos. Ao contrário da soma dos inversos dos números primos que, como vimos anteriormente na demonstração de Euler, diverge. Veja em (WIKIPéDIA, 2016).

2.4 TESTE DE PRIMALIDADE

Assim como ter funções que geram números primos é algo relevante e importante para a Matemática, testar se um determinado número é primo também é. Os números primos são estudados pelos matemáticos desde a antiguidade. Além da relevância na Matemática, os números primos se mostraram de grande importância na Ciência da Computação nas últimas décadas. Na criptografia RSA, precisamos usar números primos grandes. Com isso, é importante termos algoritmos que digam se um determinado número é primo ou não.

Veremos nesse capítulo alguns testes de primalidade, testes que afirmam se um determinado número inteiro é primo ou não. Esses testes são divididos em dois tipos: *determinísticos* e *não determinísticos*. Como estamos interessados nos algoritmos do ponto de vista matemático e computacional, comentaremos se ele é eficiente ou não, mas não aprofundaremos muito nos cálculos para justificar a eficiência.

As definições e teoremas referentes à parte de congruência que serão apresentadas de agora em diante podem ser encontradas no apêndice Congruências.

2.4.1 Custo de um algoritmo

O custo de um algoritmo é o tempo que se gasta para executá-lo. Para calcular o custo dos algoritmos nessa dissertação levaremos em conta a quantidade de operações elementares necessárias para executá-lo. Sempre que falamos em algoritmo, nossa intenção é implementá-lo em um computador. Logo, assumiremos que os números estão escritos na base 2, ou seja, são binários. Cada algarismo de um número nessa base é chamado de bit. Note que os possíveis valores para um bit é 0 ou 1. Iremos analisar duas operações específicas: adição e multiplicação.

Adição

Sejam $a = (a_{k-1}, ..., a_1, a_0)_2$ e $b = (b_{k-1}, ..., b_1, b_0)_2$ as representações binárias dos inteiros a e b. Assim cada a_i e cada b_i é 0 ou 1 e

$$a = a_{k-1}2^{k-1} + ... + a_1 2 + a_0$$

e

$$b = b_{k-1}2^{k-1} + ... + b_1 2 + b_0.$$

Para efetuarmos a soma, procedemos da maneira usual, começando por $a_0 + b_0$. Essa soma pode resultar em 0, 1 ou 2, sendo que, quando resultar em 2, devemos colocar o resultado sendo 0 e acrescentar 1 na próxima soma. Esse 1 que é acrescentado chama-se *reserva*. A próxima soma deve ser de $a_1 + b_1$ ou $a_1 + b_1 + 1$, dependendo da reserva que tivermos. Devemos proceder de forma análoga para as demais somas. Observe que, para cada reserva igual 1, aumentamos uma operação de adição. Desta forma, não conseguimos prever quantas operações faremos na adição, mas sabemos que o máximo de operações será $2k$.

Multiplicação

Usando os mesmos a e b, precisamos primeiro multiplicar b por cada bit de a e em seguida somar os resultados. Assim como na adição, na multiplicação também pode haver reservas. Teremos então k produtos e no máximo $k-1$ reservas, assim, o máximo de operações seria $2k-1$. Portanto, para calcular o produto de b por cada bit a, teremos, no máximo, $k.(2k-1)$ operações. Resta agora somarmos esses produtos, ou seja, se

$$ba_i = (c_{i,k+1}, ..., c_{i,1}, c_{i,0})_2$$

então podemos escrever a soma da seguinte maneira:

$$\begin{array}{ccccccc} & & & c_{0,k+1} & \cdots & c_{0,1} & c_{0,0} \\ & & c_{1,k+1} & \cdots & c_{1,1} & c_{1,0} & \\ & c_{2,k+1} & \cdots & c_{2,1} & c_{2,0} & & \\ & \vdots & \vdots & \vdots & & & \\ c_{k,k+1} & \cdots & c_{k,0} & & & & \end{array}$$

Sabemos que número máximo de soma em cada grandeza é de $2k$ e, como temos k grandezas, o custo dessas somas não excederá $2k^2$. Assim, a multiplicação terá $k.(2k-1)+2k^2 = 4k^2 - k$ operações.

Segundo (COUTINHO, 2004), a prática corrente é se concentrar na maior potência de k que aparece na expressão. Usaremos a notação O para determinar o custo de um algoritmo. Sejam f e g duas funções cujo domínio é $\mathbb{N}$ ou $\mathbb{R}$ e o contradomínio é $\mathbb{R}$. Dizemos que $f(x)$ é $O(g(x))$ se existirem constantes C_1 e C_2, tais que $f(x) \leq C_1 g(x)$ quando $x > C_2$. Por exemplo, seja $f(x)$ um polinômio de grau n com coeficientes reais. Então, $f(x)$ é $O(x^n)$. Assim, a soma de dois números de k bits tem custo $O(k)$ e a multiplicação tem custo $O(k^2)$. Como um inteiro positivo n tem, aproximadamente, $\log_2 n$ bits, podemos calcular o custo da soma de dois inteiros menores ou iguais a n como $O(\log_2 n)$ e a multiplicação com custo $O((\log_2 n)^2)$.

Dizemos que um algoritmo é polinomial se o número de operações que ele executa é $O((\log_2 n)^r)$, para algum $r > 0$. E o algoritmo é exponencial se o número de operações é da ordem $O(2^{\log_2 n})$ ou maior. Algoritmos polinomiais são considerados eficientes, pois são rápidos; já os exponenciais são lentos, sendo então considerados ineficientes.

2.4.2 Testes determinísticos

O primeiro tipo de testes que estudaremos será o determinístico. São chamados assim por se tratarem de testes cujo resultado nos diz se um número é primo ou composto com a garantia de que a resposta está correta. A seguir, apresentaremos alguns deles.

2.4.2.1 Crivo de Erastótenes

Com certeza você já deve ter ouvido sobre o Crivo de Erastótenes. Esse foi o primeiro método para encontrar números primos em um determinado intervalo e/ou verificar se um número é primo ou composto.

Como o Crivo de Erastótenes funciona?

Vejamos um exemplo prático: se quisermos encontrar todos os números primos menores do que 40 devemos, primeiramente, escrever todos os números de 2 a 40.

	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

Em seguida, devemos eliminar todos os múltiplos de 2, exceto ele mesmo.

Tabela 2.1 – Eliminação dos múltiplos de 2

	2	3		5		7	
9		11		13		15	
17		19		21		23	
25		27		29		31	
33		35		37		39	

Agora, devemos eliminar os múltiplos de 3 e em seguida os múltiplos de 5.

Tabela 2.2 – Eliminação dos múltiplos de 3

	2	3		5		7	
		11		13			
17		19				23	
25				29		31	
		35		37			

Tabela 2.3 – Eliminação dos múltiplos de 5

	2	3		5		7	
		11		13			
17		19				23	
				29		31	
				37			

Pela lógica, neste momento, eliminaríamos os múltiplos de 7, mas como podemos ver nenhum dos números restantes é múltiplo de 7. O mesmo ocorre para os outros valores que ainda estão na Tabela 2.3.

Portanto, os números que aparecem na Tabela 2.3 são considerados primos e os que foram eliminados são considerados compostos.

E como proceder se quisermos determinar se um dado número é primo? Vejamos o seguinte teorema:

Teorema 2.28 *Se n não é primo, então n possui um fator primo menor ou igual a* $\sqrt{n}$.

Demonstração: Seja n um número composto, tal que $n = a.b$, $a, b \in \mathbb{N}$, com $1 < a \leq b < n$. Suponhamos por absurdo que

$$a > \sqrt{n} \quad e \quad b > \sqrt{n}.$$

Assim,

$$n = a.b > \sqrt{n}.\sqrt{n} = n,$$

absurdo.

Portanto, pelo menos um fator de n deve ser menor que $\sqrt{n}$. E pelo Teorema 2.6, esse fator pode ser decomposto em um produto de números primos, todos menores ou iguais a $\sqrt{n}$.

■

Pelo teorema anterior, concluímos que, para saber se um número n é primo, devemos calcular o resto da divisão de n por cada número primo m com $2 \leq m \leq \sqrt{n}$. Se algum dos restos for 0 então n é composto, caso contrário, n é primo. Vejamos alguns exemplos:

Exemplo 2.29 *57 é um número primo?*

Primeiramente, calculamos o maior inteiro menor que $\sqrt{57}$*, ou seja,* $N < \sqrt{57} = 7,549\ldots$. *Assim basta verificarmos se 57 é divisível pelos números primos menores ou iguais a 7. Facilmente, verificamos que 57 é divisível por 3. Portanto, 57 é um número composto.*

Exemplo 2.30 *149 é um número primo?*

Devemos verificar se 149 é divisível por algum primo menor que $\sqrt{149}$*, ou seja, se 149 é divisível por 2, 3, 5, 7 ou 11. Simples divisões nos mostram que 149 não é divisível por nenhum desses números primos. Portanto 149 é um número primo!*

O *Crivo de Erastótenes* nos garante com certeza tanto se um número é primo quanto se é composto. O inconveniente desse método é que, para um número grande, ele necessita que

muitas operações sejam executadas, apresentando um custo exponencial. Computacionalmente falando, para um número com duzentos algarismos, teríamos que fazer em torno de 10^{100} divisões. Se considerarmos que, para realizar cada operação de divisão o computador leva um segundo, o tempo para determinar se um número com 200 algarismo é primo poderia chegar a ordem de 10^{92} anos. O que torna inviável o uso desse algoritmo.

2.4.2.2 Teorema de Wilson

Enunciaremos e demonstraremos um teorema que foi atribuído a Wilson (1741 - 1793), mas que anteriormente também foi provado por Lagrange (1736 - 1813). Esse teorema, conhecido como Teorema de Wilson, nos dá um critério de primalidade. Para números primos pequenos, esse critério é muito útil. Infelizmente, para primos maiores, não é eficiente.

Proposição 2.31 *Sejam $a,m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1$ mod m possui solução se, e somente se, $(a,m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é um solução, então x é uma solução da congruência se, e somente se, $x \equiv x_0$ mod m.*

A demonstração dessa proposição pode ser encontrada em (HEFEZ, 2016), página 194.

Teorema 2.32 *Um número p é primo se, e somente se, $(p-1)! \equiv -1 \quad mod\ p$.*

Demonstração: ($\Rightarrow$) Para $p = 2$ e $p = 3$, o resultado segue de imediato. Suponhamos $p \geq 5$ primo. Para todo $i \in \{1,...,p-1\}$, segue da Proposição 8 do apêndice Congruências que a congruência $iX \equiv 1$ mod p possui uma única solução módulo p. Assim, dado $i \in \{1,...,p-1\}$, existe um único $j \in \{1,...,p-1\}$ tal que $ij \equiv 1$ mod p. Por outro lado, se $i \in \{1,...,p-1\}$ é tal que $i^2 \equiv 1$ mod p, então $p|i^2-1$, ou seja, $p|i-1$ ou $p|i+1$, o que só pode ocorrer se $i = 1$ ou $i = p-1$. Logo,

$$2...(p-2) \equiv 1 \quad mod\ p,$$

e, portanto,

$$1.2...(p-2).(p-1) \equiv p-1 \equiv -1 \quad mod\ p.$$

($\Leftarrow$) Suponhamos que $(p-1)! \equiv -1\ mod p$, ou seja, $p|((p-1)!+1)$. Queremos mostrar que p é um número primo. Suponhamos que $p = a.b$, com $a \neq p$. Assim, $a|((p-1)!+1)$. Como a é um dos fatores de $(p-1)!$, temos que $a|(p-1)!$ e consequentemente $a|1$, ou seja, $a = 1$. Implicando assim que p é um número primo.

■

2.4.2.3 Teste de Lucas

Édouard Lucas, matemático francês, muito conhecido por suas recreações matemáticas, como por exemplo a famosa *Torre de Hanói*, também contribuiu com muitos resultados da teoria dos números. Uma de suas contribuições foi o teste de primalidade conhecido como *Teste de Lucas* que nos afirma com certeza se um número é primo. Saiba mais em: https://mathshistory.st-andrews.ac.uk/Biographies/Lucas/

Além da congruência, ele utiliza a função $\phi(n)$ para determinar se n é um número primo. O teste parte da ideia de que se $\phi(n) = n-1$, então n é primo. Essa ideia vem do fato que se existem $n-1$ números menores do que n cujo máximo divisor comum entre cada um desses números com n é igual a 1, então n é primo.

Teste de Lucas: *Seja $n \in \mathbb{N}$ um número ímpar e $2 \leq b \leq n-1$ um inteiro. Temos que n será um número primo se*

$$b^{n-1} \equiv 1 \quad mod\ n \tag{2.9}$$

e

$$b^{\frac{n-1}{p}} \not\equiv 1 \quad mod\ n \tag{2.10}$$

para todos fatores primos p de $n-1$.

O *Teste de Lucas* não apresenta uma maneira de escolhermos a base b. Caso não obtenhamos um resultado satisfatório com a base escolhida, devemos mudá-la e repetir o teste.

Devemos estar atentos a afirmação do teste. Ele nos diz que se as condições anteriores forem satisfeitas, n é um número primo. No entanto, nada podemos afirmar se as condições não forem satisfeitas.

Exemplo 2.33 *1031 é um número primo?*

Primeiramente devemos escolher a base, $b = 2$. Em seguida, encontrarmos os fatores primos de $1031 - 1 = 1030 = 2.5.103$.

Restando apenas testar as congruências.

$$2^{1030} \equiv 1 \quad mod\ 1031$$

$$2^{1030/2} \not\equiv 1 \quad mod\ 1031$$

$$2^{1030/5} \not\equiv 1 \quad mod\ 1031$$

$$2^{1030/103} \not\equiv 1 \quad mod\ 1031$$

A primeira congruência satisfaz a condição (2.9) e as outras três satisfazem a condição (2.10).

Portanto, podemos afirmar com certeza que 1031 é um número primo.

Exemplo 2.34 *143 é um número primo?*

Escolhendo a base, $b = 2$, vamos encontrar os fatores primos de $143 - 1 = 142 = 2.71$.

Restando apenas testar as congruências.

$$2^{142} \equiv 114 \quad mod\ 143$$

$$2^{142/2} \not\equiv 1 \quad mod\ 143$$

$$2^{142/71} \not\equiv 1 \quad mod\ 143$$

As duas últimas congruências satisfazem as condições do teste, mas a primeira, não. Desta forma o teste fica inconclusivo. Nossa única conclusão é que o número 143 pode ser composto ou que escolhemos uma base que não foi satisfatória.

Ao analisarmos a congruência (2.10), percebemos que ela deve ser verificada para todos os fatores primos de $n-1$, em outras palavras, devemos fatorar $n-1$. No último exemplo que demos, é fácil fatorar 142, mas quando se trata de números grandes, essa fatoração se torna inviável. E piora ainda mais se tivermos que trocar a base e refazer o teste.

2.4.2.4 Teste Lucas-Lehmer

Apresentaremos agora um teste que auxilia na descoberta dos primos de Mersenne, o *Teste de Lucas-Lehmer*. Esse teste possui um algoritmo de fácil execução e custo polinomial e graças a ele os maiores primos conhecidos são os de Mersenne. Este teste foi desenvolvido por Lucas (1876) e posteriormente melhorado por Derrick Henry Lehmer (1930).

Teorema 2.35 ***(Teste de Lucas-Lehmer)*** *Para todo número natural n, o número de Mersenne, $M_n = 2^n - 1$ é primo se, e somente se, $S_{n-2} \equiv 0\ mod\ M_n$, sendo $S_n = S_{n-1}^2 - 2$ e $S_0 = 4$.*

Na seção sobre os *primos de Mersenne*, vimos que nem todos os números de Mersenne são primos. Vejamos alguns exemplos usando o Teste de Lucas-Lehmer.

Exemplo 2.36 *$M_5 = 31$ é um número primo?*

Devemos verificar se $S_3 \equiv 0$ mod 31. Sabemos que $S_0 = 4$, assim

$$S_1 = 4^2 - 2 = 14,$$

$$S_2 = 14^2 - 2 = 194 \equiv 8 \quad mod\ 31;$$

$$S_3 \equiv 8^2 - 2 = 64 \equiv 0 \quad mod\ 31.$$

Portanto, pelo Teste de Lucas-Lehmer, o número de Mersenne, M_5, é um número primo.

Exemplo 2.37 *$M_{11} = 2047$ é um número primo?*

Levando em consideração a Proposição 2.3.3, como 11 é um número primo, M_{11} é um forte candidato a ser primo também. Precisamos verificar se $S_9 \equiv 0$ mod 2047. Usando o mesmo raciocínio do exemplo anterior e $S_0 = 4$, temos:

$$S_1 = 4^2 - 2 = 14,$$

$$S_2 = 14^2 - 2 = 194;$$

$$S_3 = 194^2 - 2 \equiv 788 \quad mod\ 2047.$$

$$S_4 \equiv 788^2 - 2 \equiv 701 \quad mod\ 2047.$$

$$S_5 \equiv 701^2 - 2 \equiv 119 \quad mod\ 2047.$$

$$S_6 \equiv 119^2 - 2 \equiv 1877 \quad mod\ 2047.$$

$$S_7 \equiv 1877^2 - 2 \equiv 240 \quad mod\ 2047.$$

$$S_8 \equiv 240^2 - 2 \equiv 282 \quad mod\ 2047.$$

$$S_9 \equiv 282^2 - 2 \equiv 1736 \quad mod\ 2047.$$

Como a última congruência não satisfaz o Teste de Lucas-Lehmer, concluímos que M_{11} não é um número primo.

2.4.2.5 Fatoração de Fermat

Sabemos, pelo Teorema 2.6, que todo número composto pode ser fatorado, mas nem sempre essa fatoração é simples e viável. Ela só é eficiente quando estamos trabalhando com números pequenos. Veremos agora a *Fatoração de Fermat*, um algoritmo que, segundo (COUTINHO, 2009) é muito eficiente quando o número n tem um fator primo próximo de $\sqrt{n}$.

Todo número inteiro ímpar n pode ser escrito como a diferença do quadrado de dois números, ou seja, $n = 2k+1 = (k+1)^2 - k^2$. Deste modo, o algoritmo consiste em achar números inteiros positivos x e y tais que

$$n = x^2 - y^2 = (x+y).(x-y),$$

desta forma $(x+y)$ e $(x-y)$ são os fatores de n.

Mas como encontrar esses inteiros x e y?

Encontraremos o valor inicial de x, que será o maior inteiro menor que $\sqrt{n}$. Note que se $\sqrt{n}$ for um número inteiro, então teremos $x = \sqrt{n}$ e $y = 0$. Sendo assim, n é um número composto e a fatoração está feita. Caso contrário, devemos incrementar x de um em um e calcular $y = \sqrt{x^2 - n}$ até que y seja um número inteiro ou $x = \dfrac{n+1}{2}$. Se ocorrer o primeiro caso, n é composto. Do contrário, n é primo. Vejamos agora dois exemplos para facilitar a compreensão da Fatoração de Fermat.

Exemplo 2.38 *259 é um número primo ou composto?*

Primeiro verificamos se 259 é um quadrado perfeito. Como $\sqrt{259}$ *é aproximadamente 16,09, concluímos 259 não é um quadrado perfeito. Temos que o valor de x é inicialmente igual ao menor inteiro maior que* $\sqrt{259}$*, assim* $x = 17$*. Em seguida devemos calcular o valor de y. Repetiremos esse passo até que y seja um número inteiro ou* $x = \dfrac{n+1}{2}$.

Veja a seguinte tabela:

x	y
17	5,47
19	10,09
20	11,87
21	13,49
22	15

Assim, $259 = (22+15)\cdot(22-15) = 37\cdot 7$*. Portando 259 é um número composto.*

Exemplo 2.39 *41 é um número primo?*

Inicialmente temos $x = 6$. *Novamente, como* $\sqrt{41}$ *não é um número exato, devemos adicionar 1 ao x e calcular o valor de y. Veja a tabela:*

x	y
7	1,41
8	4,12
9	5,83
10	7,68
...	...
20	18,94
21	20

Logo, $41 = (21+20)\cdot(21-20) = 41\cdot 1$. *Portanto, 41 é um número primo.*

Observe que 41 é um número pequeno e mesmo assim precisamos de 15 passos para efetuar a fatoração de Fermat. Isso nos mostra que, apesar da fatoração sempre funcionar, ela possui um custo exponencial. De acordo com o que vimos, a Fatoração de Fermat não é eficiente. Porém, quando n possui dois fatores próximos, esse algoritmo é eficiente para encontrá-los. Para descobrir porque o algoritmo funciona, veja capítulo 2, seção 5 de referência (COUTINHO, 2004).

2.4.2.6 AKS

Veremos agora uma das grandes conquistas na parte de testes de primalidade, o *Teste AKS*. Trata-se de um teste determinístico e ao mesmo tempo tem custo polinomial. Foi criado e publicado por Manindra **A**grawal, Neeraj **K**ayal e Nitin **S**axena, cientistas indianos. Veja a publicação em (AGRAWAL; KAYAL; SAXENA, 2004).

Assim como vários testes apresentados nessa dissertação, o *Teste AKS* também se baseia no Pequeno Teorema de Fermat. Vejamos o fundamento matemático do AKS. Seja x uma variável, a um inteiro e p um número primo. Pelo binômio de Newton temos que:

$$(x+a)^p = \sum_{j=0}^{p} \binom{p}{j} x^{p-j} a^j$$

mas, quando j é diferente de 1 e p, o coeficiente binomial $\binom{p}{j}$ é divisível por p, assim

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

usando o Pequeno Teorema de Fermat para a última equivalência.

Reciprocamente, se

$$(x+a)^N \equiv x^N + a \mod N$$

para todo $a < N$, então tomando $a = 1$, temos que N divide todos os coeficientes binomiais $\binom{N}{j}$ com $0 < j < N$.

Suponhamos N composto e seja q um de seus fatores primos. Então

$$\binom{N}{q} = \frac{N(N-1)...(N-q+1)}{q(q-1)...1}.$$

Nessa expressão temos que apenas N e q são divisíveis por q. Assim, se q^k é a maior potência, de q, que divide N então $q^k \nmid \binom{N}{q}$, logo $N \nmid \binom{N}{q}$, o que é um absurdo. Portanto N é primo.

Obtemos então, o seguinte critério de primalidade:

$$N \text{ é primo} \Leftrightarrow (x+a)^N \equiv x^N + a \ \ (mod\ N), \text{ para todo } a < N$$
$$\Leftrightarrow (x+a)^N \equiv x^N + a \ \ (mod\ N), \text{ para algum } a < N, \text{ com } mdc(a,N) = 1.$$

Como podemos notar, este critério é ineficiente, pois devemos calcular todos os coeficientes de $(x+a)^N$ e mostrar que os coeficientes intermediários são divisíveis por N. No entanto, se $(x+a)^N \equiv x^N + a \ \ mod\ N$, então eles deixam o mesmo resto módulo N quando divididos por qualquer polinômio. Um caso particular seria pegar esse polinômio igual a $x^r - 1$, assim

$$\text{N é primo} \Rightarrow (x+a)^N \equiv x^N + a \ \ (mod\ x^r - 1, N), \text{ para todo } a < N \text{ e } r \in \mathbb{N}.$$

O que os cientistas indianos mostraram foi que, para garantir que N seja primo, precisamos testar apenas se a congruência é válida para um valor específico de r, dependente polinomialmente de $\log N$, e alguns valores de a.

Definição 2.40 *Se $a, n \in \mathbb{Z}$ com $mdc(a,n) = 1$, definimos a ordem de a módulo n como sendo o menor $l \in \mathbb{N}^*$ tal que $a^l \equiv 1 \ \ mod\ n$, denotamos l por $ord_n a$*

Algoritmo AKS

O algoritmo AKS se divide em sete etapas:

1ª etapa: Entrada $N > 6$.

2ª etapa: Se $N = a^b$, com $b > 1$, retorna COMPOSTO.

3ª etapa: Encontrar o menor r tal que $ord_r N > \frac{1}{2}(\log_2 N)^2$.

4ª etapa: Se $mdc(a,N) > 1$ para algum primo $a \leq r$, retorna COMPOSTO.

5ª etapa: Se $\sqrt{N} < r$, retorna PRIMO.

6ª etapa: Para $a = 1$ até $\lfloor \sqrt{\phi(r)/2} \log_2 N \rfloor$ faça

Se $(x+a)^N \not\equiv x^N + a \ \ (mod\ x^r - 1, N)$, retorna COMPOSTO.

7º etapa: Retorna PRIMO.

Vejamos agora dois exemplo para o AKS.

Exemplo 2.41 *213 é um número primo?*

1ª etapa: N = 213

2ª etapa: $213 \neq a^b$.

3ª etapa: Sendo $l = ord_r 213$*, devemos encontrar o menor r tal que*

$$213^l \equiv 1 \ \ mod\ r, \text{ sendo } l > \tfrac{1}{2}(\log_2 213)^2 \cong 29,96.$$

Temos que $l = 31$ *e* $r = 3$.

4ª etapa: $mdc(3,213) = 3$*, retorna COMPOSTO.*

Portanto, 213 é um número composto.

Exemplo 2.42 *47 é um número primo?*

1ª etapa: $N = 47$.

2ª etapa: $47 \neq a^b$.

3ª etapa: Sendo $l = ord_r 47$*, devemos encontrar o menor r tal que*

$$47^l \equiv 1 \ \ mod\ r, \text{ sendo } l > \tfrac{1}{2}(\log_2 47)^2 \cong 15,43.$$

Temos que $l = 18$ *e* $r = 5$.

4ª etapa: $mdc(2,47) = 1$*,* $mdc(3,47) = 1$ *e* $mdc(5,47) = 1$.

5ª etapa: $\sqrt{47} \cong 6,8556 > 5$*, não podemos afirmar nada.*

6ª etapa: Primeiramente, devemos calcular $\lfloor \sqrt{\phi(5)/2} \log_2 47 \rfloor = 7$*. Faça* $(x+a)^{47}$*, para todo* $1 \leq a \leq 7$*, e verifique se é congruente a* $(x^{47} + a)$ *módulo* $(x^5 - 1, 47)$*. Temos que a congruência é verdadeira para todo* $1 \leq a \leq 7$.

7ª etapa: retorna PRIMO.

Portando, 47 é um número primo.

2.4.3 Testes não determinísticos

Veremos agora o segundo tipo de teste: não determinísticos. Segundo (COUTINHO, 2004), esses testes também nos diz se um determinado número é primo, mas dentro de uma margem de erro. Vejamos alguns:

2.4.3.1 Teste de Leibniz

Leibniz, matemático alemão, foi quem deu o ponta pé inicial aos testes de primalidade. Apesar de seu teste não estar totalmente correto, auxiliou para que muitos matemáticos tivessem um ponto de partida e conseguissem aperfeiçoá-lo.

Leibniz tinha como base o *Pequeno Teorema de Fermat*. Ele acreditava que a recíproca do teorema também era verdadeira, ou seja, se $p|a^{p-1}-1$, sendo $mdc(a,p)=1$, então p é primo. Para facilitar os calculos, Leibiniz sempre utilizava $a=2$.

Teste de Leibniz: *Dado um número ímpar $n \in \mathbb{N}$, se $2^{n-1} \equiv 1$ mod n, então n é primo.*

Leibniz não fez uma demonstração para essa sua suposição. Infelizmente, nem sempre essa afirmação está correta. O teste nos diz com certeza se um determinado número é composto, mas quando o teste nos afirma que n é primo, não é com certeza e sim com uma grande possibilidade que seja.

Vejamos alguns exemplos:

Exemplo 2.43 *131 é um número primo?*

Usando o teste de Leibniz, temos que:

$$2^{130} \equiv 1 \quad mod\ 131$$

Portanto, segundo o teste, 131 é um número primo.

Mas não podemos afirmar, com certeza, que 131 é um número primo. Com o auxilio de uma calculadora científica conseguimos verificar que essa congruência está correta e que 131 realmente é um número primo.

Exemplo 2.44 *561 é um número primo?*

Usando o teste de Leibniz, encontramos a seguinte congruência:

$$2^{560} \equiv 1 \quad mod\ 561$$

Portanto, segundo o teste, 561 é considerado um número primo.

Como 561 é um número pequeno, conseguimos fatorá-lo com facilidade e perceber que $561 = 3 \cdot 11 \cdot 17$. Logo, 561 é um número composto.

Pelos exemplos anteriores conseguimos perceber que o *Teste de Leibniz* ora acerta, ora erra. Vejamos mais um exemplo:

Exemplo 2.45 *407 é um número primo?*

Usando o teste de Leibniz, encontramos a seguinte congruência:

$$2^{406} \equiv 284 \quad mod\ 407$$

Assim, como 2^{406} *não é congruo a 1 mod 407, podemos afirmar com certeza que 407 é um número composto.*

Vimos, com esse último exemplo, que a congruência não foi satisfeita, assim podemos afirmar com certeza que o número 407 é composto.

Curiosidade: Leibniz foi um grande contribuinte para o campo das calculadoras mecânicas. Foi ele quem adicionou a multiplicação, a divisão e a raiz quadrada na calculadora de Pascal. Inventou uma *Calculadora de Pisar*, que usava uma engrenagem cilíndrica para pisar e essa invenção acabou influenciando Thomas Arithmometer a criar a primeira calculadora mecânica produzida em grande escala. Leibniz também refinou o sistema de números binários que é a base de todos os computadores digitais. Veja em (WIKIPéDIA, 2020a).

2.4.3.2 Teste de Miller-Rabin

Gary L. Miller, atualmente, é professor de Ciência da Computação em *Carnegie Mellon University*, nos Estados Unidos e ainda contribui muito com a área da computação. Michael Rabin, conhecido por suas contribuições inovadoras na área da ciência da computação, trabalhou com criptografia e números primos. Mas o que ressaltaremos aqui é a influência de ambos no teste de primalidade conhecido como *Teste Miller-Rabin*.

Como dissemos anteriormente, o *Teste de Leibniz* serviu como base para que outros matemáticos o aprimorassem e aumentassem sua precisão. Miller e Rabin foram dois deles. O *Teste de Miller-Rabin*, possui algumas condições a serem verificadas. No entanto, se as

condições forem satisfeitas, há uma grande possibilidade do número ser primo, mas não uma certeza.

Originalmente, o teste foi desenvolvido por Miller e era um teste determinístico. Porém, esse teste era baseado na Hipótese de Riemann estendida que ainda não foi demonstrada. Foi então que Rabin fez uma alteração no teste tornando-o não determinístico. Rabin demonstrou que a probabilidade de erro a cada execução era de no máximo $\frac{1}{4}$, sendo que na média esse número é bem menor.

Teorema 2.46 *Seja $n \in \mathbb{N}$ um número ímpar e $1 < b < n-1$, um inteiro. Como n é ímpar temos que $n-1$ é um par. Portanto pode ser escrito como $n-1 = 2^k \cdot q$, sendo k o maior expoente possível do 2 e, consequentemente, q um número ímpar. Temos então que n é primo se algum*

$$b^q, b^{2q}, b^{2^2 q}, ..., b^{2^{k-1} q} \equiv -1 \quad mod\ n$$

$$ou$$

$$b^{2^k q} \equiv 1 \quad mod\ n.$$

Demonstração: Considere as seguintes potências $b^q, b^{2q}, b^{2^2 q}, ..., b^{2^{k-1} q}, b^{2^k q}$. Se n é um número primo, usando o *Pequeno Teorema de Fermat* temos que $b^{2^k q} = b^{n-1} \equiv 1$ mod n. Temos então que pelo menos uma das potências de b é congruente a 1 módulo n. Seja $s \geq 1$ o menor expoente tal que $b^{2^s q} \equiv 1$ mod n, assim:

$$b^{2^s q} - 1 = (b^{2^{s-1} q} - 1) \cdot (b^{2^{s-1} q} + 1).$$

Logo,

$$n | (b^{2^{s-1} q} - 1)$$

$$\text{ou}$$

$$n | (b^{2^{s-1} q} + 1)$$

Como s era o menor expoente que satisfazia a congruência, temos que $(b^{2^{s-1} q} - 1)$ não é divisível por n. Portanto $n | (b^{2^{s-1} q} + 1)$, ou seja,

$$b^{2^{s-1} q} \equiv -1 \quad mod\ n,$$

sendo $1 \leq s-1 \leq k-1$.

■

O desejo de muitos matemáticos é que a recíproca do terorema acima fosse verdadeira, porque teríamos um teste determinístico eficiente. Porém, a recíproca não é verdadeira. Mas, mesmo assim podemos usar a recíproca para obter um teste de probabilidade eficiente. Esse novo teste não é determinístico e sim probabilístico.

Definição 2.47 *Seja $n \in \mathbb{N}$ um número composto ímpar, com $n-1 = 2^{kq}$. Dizemos que n é um pseudoprimo forte na base a se ou $a^q \equiv 1 \mod n$ ou existe $j' < k$ com $(a^q)^{2^{j'}} \equiv -1 \mod n$.*

Existem infinitos pseudoprimos forte em qualquer base $a > 1$.

Definição 2.48 *Seja A um conjunto finito. Denotamos a quantidade de elementos de A por #A.*

Teorema 2.49 *Seja*

$$\alpha(n) = \frac{\#\{a|\ 0 < a < n,\ n\ \ um\ pseudoprimo\ forte\ na\ base\ a\}}{\phi(n)}.$$

Então, para todo número composto ímpar $n > 9$, temos que $\alpha(n) \leq \frac{1}{4}$.

A demonstração desse teorema poder ser encontrada em (MARTINEZ; SALDANHA; TENGAN, 2011).

Usando o teorema acima podemos desenvolver alguns testes de primalidade probabilísticos, como o chamado de *Teste de Miller-Rabin*.

Teste de Miller-Rabin

Dado $n \in \mathbb{N}$, com n ímpar e $n > 9$, tome t valores de a tais que $1 < a < n$. Verifique para cada a se

$$a^q, a^{2q}, a^{2^2 q}, ..., a^{2^{k-1} q} \not\equiv -1 \mod n$$

e

$$a^{2^k q} \not\equiv 1 \mod n.$$

Se as condições acima forem verificadas a é composto. Caso contrário, com probabilidade $\left(\frac{1}{4}\right)^t$, temos que n é primo.

Vejamos agora dois exemplos para o Teste de Miller-Rabin.

Exemplo 2.50 *241 é um número primo?*

Sabemos que $n = 241$, então $n - 1 = 240 = 2^4.15$

Assim, $k = 4$, $q = 15$ e escolhendo $b = 2$ e $t = 1$ para facilitarmos as contas, temos as seguintes congruências:

$$2^{15} \equiv 233 \quad mod\ n$$

$$2^{2.15} \equiv 64 \quad mod\ n$$

$$2^{2^2.15} \equiv 240 \equiv -1 \quad mod\ n \tag{2.11}$$

$$2^{2^3.15} \equiv 1 \quad mod\ n$$

$$2^{2^4.15} \equiv 1 \quad mod\ n \tag{2.12}$$

Pelas congruências 2.11 e 2.12, o Teste de Miller-Rabin nos diz que 241 é primo.

Como o teste de Miller-Rabin não é determinístico, não podemos afirmar com certeza que 241 é um número primo, mas sim que há uma grande chance de ser. Com o auxílio de uma calculadora é fácil comprovar que 241 é realmente um número primo.

O próximo exemplo nos garante com certeza que o número testado é composto.

Exemplo 2.51 *247 é um número primo?*

Como $n = 247$, temos que $n - 1 = 246 = 2.123$

Assim, $k = 1$ e $q = 123$ e escolhendo a base $b = 2$ temos:

$$2^{123} \equiv 164 \quad mod\ 247$$

$$2^{2.123} \equiv 220 \quad mod\ 247$$

Pelas congruências acima podemos afirmar com certeza que 247 é um número composto.

A escolha da base é importante para chegarmos a uma conclusão, por isso, ao testarmos mais de uma base, conseguimos diminuir os possíveis erros. Alguns *softwares* usam 10 bases diferentes para tentarem minimizar erros.

2.5 PROBLEMAS EM ABERTO

Apesar de serem estudados há muito tempo, ainda existem conjecturas sobre os números primos que não foram demonstradas. Vejamos algumas delas:

Primos de Fermat

Como vimos na seção *Primos especiais*, sabemos que os *Primos de Fermat*, são números da forma

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, ...$$

que são primos.

Em uma de suas cartas, modo como discutia suas descobertas matemáticas, Fermat sugere que esses números são sempre primos. O que de fato acontece quando $n = 0, 1, 2, 3, 4$. Posteriormente, Euler (1732) mostrou que para $n = 5$ o número de Fermat era composto, contrariando a hipótese de Fermat. Até os dias atuais, não se sabe da existência de outros números de Fermat primos além dos cinco primeiros.

Primos gêmeos

Como vimos anteriormente, *Primos gêmeos* são primos da forma p e p+2. Sabemos que todo número inteiro pode ser escrito como $6k$, $6k-1$, $6k-2$, $6k+1$, $6k+2$, $6k+3$, sendo o $6k-1$ e $6k+1$ os únicos que podem ser primos. Além disso, a diferença entre eles é 2. Pelo teorema de Dirichlet existem infinitos primos da forma $6k-1$ e $6k+1$, $k \in \mathbb{Z}$ e cada par de primos gêmeos pode ser escrito como $(6k-1, 6k+1)$, exceto $(3, 5)$. Podemos concluir, então, que existem infinitos primos gêmeos? Ou seja, existem infinitos pares de números da forma $(p, p+2)$?

Essa pergunta é uma famosa conjectura dos números primos gêmeos e ainda está em aberto e é um dos temas centrais da moderna teoria analítica dos números.

Infelizmente, mostrar que os primos gêmeos são da forma $(6k-1, 6k+1)$ não garante que todos os números da forma $6k-1$ ou $6k+1$ são primos, ou seja, a recíproca não é verdadeira.

Com os trabalhos de Zhang e Maynard, vistos anteriormente, ficamos cada vez mais otimistas em encontrar uma demonstração para essa conjectura.

Primos de Sophie Germain

Com relação aos *primos de Sophie Germain* não se sabe se são infinitos, mas também nunca foi provado o contrário, desta forma, conjectura-se que existam infinitos números primos de Sophie Germain.

3 CRIPTOGRAFIAS

Uma das perguntas mais frequentes que todos os professores ouvem é: “Onde eu vou usar isso?”. Um exemplo prático e que faz parte do cotidiano dos alunos é a criptografia. E poder mostrar que, graças a Matemática e os números primos, é possível ter uma codificação de mensagem mais segura, faz despertar o interesse dos alunos por essa área.

Não podemos falar de criptografia sem mencionar o Código de César ou Cifra de César, um dos códigos mais antigos e mais simples que consiste em trocar as letras do alfabeto seguindo uma ordem bem determinada. O código recebe esse nome devido ao general Júlio César, do Império Romano, que o criou para se comunicar com seu exército sem que a mensagem fosse descoberta por seus inimigos.

Segundo (COUTINHO, 2009), códigos desse tipo apresentam um grande problema: são fáceis de “quebrar”, ou seja, rapidamente outra pessoa, que não seja o destinatário legítimo, consegue descobrir o código usado e ler a mensagem original. Isso ocorre devido à frequência média que cada letra aparece em uma frase ou texto. Na nossa língua as vogais são mais usadas do que as consoantes e dentre as vogais a letra *a* é a mais usada, ficando fácil identificar qual a substituição utilizada.

Vejamos um exemplo do Código de César. Primeiramente devemos ter uma tabela de conversão. No caso do general Júlio César, sua tabela consistia em trocar a letra A pela letra D, a letra B pela E e assim sucessivamente (ver (HEFEZ, 2016)). Veja a tabela a seguir:

Tabela 3.1 – Tabela de conversão

Alfabeto	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
Código	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*
Alfabeto	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
Código	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*

Assim, se quisermos codificar a mensagem original:

NÃO SE RENDA

teremos a mensagem codificada:

QDR VH UHQGD

Note que, para frases pequenas, não fica tão evidente qual a frequência média de cada letra. Segundo (COUTINHO, 2009), o método de decodificar a mensagem usando a frequência média, só funciona se a mensagem for longa.

Com o avanço da tecnologia, códigos como o de César se tornaram mais fáceis de serem quebrados e desta forma fez-se necessária a criação de códigos mais eficazes.

Os códigos mais simples utilizam o que chamamos de *criptografia de chave simétrica*, cuja chave de codificação e de decodificação é a mesma. Já os códigos mais elaborados, aqueles que são usados atualmente, utilizam a *criptografia de chave assimétrica*, na qual as chaves de codificação e decodificação são diferentes.

Veremos nesse capítulo a *Criptografia RSA*, o *Protocolo Diffie-Hellman* e a *Criptografia ElGamal*.

3.1 Criptografia RSA

Veremos agora um dos mais seguros métodos de criptografia, a *Criptografia RSA*, um código inventado por R. L. **R**ivest, A **S**hamir e L. **A**dleman quando trabalhavam no Massachussets Institute of Technology (M.I.T). Como podemos notar, **RSA** são as iniciais dos nomes dos inventores desse código.

A *criptografia RSA* consiste em um método de criptografia de chave pública que para ser implementado precisa de dois parâmetros básicos: dois números primos muito grandes e distintos. Exatamente o que faz a segurança ser extremamente eficiente, pois é difícil fatorar números primos muito grandes.

Curiosidade: Em certa ocasião, Rivest, após anos de estudo com seus amigos, ao pensar sobre o problema das cifras assimétricas imaginou que a função de mão única poderia solucionar esse problema e conseguiu formalizar sua descoberta em um artigo. Rivest assinou esse artigo colocando seu nome e dos outros dois colaboradores em ordem alfabética: Adleman, Rivest e Shamir. Por achar esse trabalho menos interessante do que os outros em que havia participado, Adleman, sugeriu colocar seu nome por último. No entanto, o Sistema RSA se tornou uma das cifras mais importantes da criptografia moderna. Ver (SINGH, 2005).

Segundo (COUTINHO, 2016), a descrição da Criptografia RSA consiste em, além de mostrar os passos para codificar e decodificar uma mensagem, verificar a autenticidade do método.

3.1.1 Pré-codificação

Primeiramente, para usarmos o método RSA, devemos converter a mensagem em números. Para simplificar, vamos supor que a nossa mensagem é constituída apenas por palavras. Para converter a mensagem em sequencia de números usaremos a seguinte tabela de conversão:

Tabela 3.2 – Tabela de conversão

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

Para representar o espaço entre as palavras, será usado o número 99. O uso de dois algarismos para cada letra evita a ambiguidade. Por exemplo, se colocássemos a letra A sendo 1, a letra B sendo 2 e assim por diante, ao colocarmos o número 12 não saberíamos se a correspondência seria AB ou L, que é a décima segunda letra do nosso alfabeto.

O próximo passo é determinarmos os números primos distintos, p e q, que usaremos como parâmetros e que será de conhecimento apenas do receptor da mensagem. A partir desses primos, determinaremos n, sendo $n = p.q$. Esse número n será de conhecimento público, o que não afeta a segurança do método desde que escolhamos p e q grandes e distantes um do outro, tornando a fatoração de n inviável. Segundo (COUTINHO, 2009), não basta p e q serem grandes se $|p-q|$ for pequeno, pois a fatoração de n se torna fácil se utilizarmos o algoritmo de fatoração de Fermat.

O último passo consiste em separar o longo número, que encontraremos na conversão, em blocos. Esses blocos não precisam ter todos a mesma quantidade de algarismos; devem, apenas, ser números menores do que n e não começar com o número zero.

Exemplo 3.1 *Seja $p = 17$ e $q = 23$, assim $n = 391$. Queremos converter a frase: Deus é fiel. Deste modo, a frase é convertida no número*

$$131430289914991518142 1.$$

Separando esse número em blocos temos:

$$1-314-302-89-91-49-91-51-8-142-1.$$

3.1.2 Codificação e decodificação

Neste momento faremos a codificação da mensagem. Para isso, necessitamos do número n e de um outro inteiro positivo e de tal forma que $mdc(e,\phi(n)) = 1$. Como $n = p.q$, determinar o valor de $\phi(n)$ é simples. Ao par (n,e) daremos o nome de *chave de codificação* do sistema RSA, que será de conhecimento público. A frase "Deus é fiel" foi convertida em blocos, os quais serão, cada um, codificados separadamente. A mensagem codificada será a sequência dos blocos codificados, sem que esses sejam reunidos.

Como codificar um bloco?

Lembre-se que todos os blocos devem ser menores do que n. Se chamarmos o bloco a ser codificado de b e o bloco codificado de $C(b)$, para encontrarmos $C(b)$ basta calcularmos o resto da divisão de b^e por n.

Em outras palavras, C(b) é a forma reduzida de b^e módulo n, mas sempre trabalhando com restos positivos.

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

Exemplo 3.2 *No Exemplo 3.1, vamos codificar o terceiro bloco: 302.*

Temos $n = 391$*, assim* $\phi(391) = \phi(17.23) = (17-1).(23-1) = 352$*. Agora, devemos escolher e. Para facilidade dos cálculos, escolheremos* $e = 3$*, sendo* $mdc(3,352) = 1$.

Todos esses valores são escolhidos e calculados pelo receptor. O emissor só terá conhecimento do números n e e que serão necessários para que ele codifique sua mensagem.

Temos então:

$$302^3 \equiv (-89)^3 \equiv -387 \equiv 4 \ mod \ 391.$$

Portanto, o bloco 302 é codificado como 4.

Codificando toda a mensagem teríamos a seguinte sequência:

$$1-155-4-387-114-349-114-102-121-386-1.$$

Decodificando a mensagem

Passemos agora para a decodificação da mensagem. Nesse momento necessitamos do número n e do inverso multiplicativo de e em $\phi(n)$, que será denotado por d. Ao par (n,d) daremos o nome de *chave de decodificação*, sendo essa de conhecimento exclusivo do receptor da mensagem. Utilizando o algoritmo euclidiano estendido podemos encontrar d de maneira fácil, veja (COUTINHO, 2009).

Seja $C(b)$ um bloco da mensagem codificada e $D(C(b))$ o resultado da decodificação. Para encontrarmos $D(C(b))$ basta calcularmos resto da divisão de $C(b)^d$ por n.

Em outras palavras, $D(C(b))$ é a forma reduzida de $C(b)^d$ módulo n.

$$D(C(b)) \equiv C(b)^d \quad mod\ n$$

Exemplo 3.3 *Faremos a decodificação do terceiro bloco: 4. Usaremos* $d = 235$ *que foi encontrado pelo algoritmo euclidiano estendido.*

Calculando D(4), referente ao terceiro bloco, temos:

$$4^{235} \equiv 302 \quad mod\ 391$$

Ou seja, decodificando 4, temos o número 302. Portanto, decodificando o bloco 4, voltamos ao bloco original.

Mas será que isso acontece para todos os blocos? Se sim, por que é válido?

3.1.3 Autenticidade do método

Precisamos mostrar que $D(C(b)) = b$. Temos que:

$$C(b) \equiv b^e \quad mod\ n \tag{3.1}$$

$$D(C(b)) \equiv C(b)^d \quad mod\ n \tag{3.2}$$

$$e.d \equiv 1 \quad mod\ \phi(n) \tag{3.3}$$

Combinando as congruências (3.1) e (3.2) , temos:

$$D(C(b)) \equiv (b^e)^d \quad mod\ n$$

$$D(C(b)) \equiv b^{e.d} \quad mod\ n \tag{3.4}$$

Queremos mostrar que

$$b^{e.d} \equiv b \quad mod\ n.$$

Pela equação (3.3), existe um inteiro k tal que :

$$ed = k\phi(n) + 1.$$

Usando a equação (3.4)

$$b^{k\phi(n)+1} \equiv D(C(b)) \quad mod\ n. \tag{3.5}$$

Dividiremos a demonstração em três casos.

Primeiro caso: $p|b$ e $q|b$. Assim, $p|b$ implica que

$$b \equiv 0 \quad mod\ p$$

então

$$b^{ed} \equiv 0 \quad mod\ p.$$

Como p é primo, temos que $p|b$.

De forma análoga, concluímos que, se $q|b$, então

$$b^{ed} \equiv 0 \quad mod\ q.$$

Como q é primo, temos que $q|b$. Dos fatos que $mdc(p,q) = 1$ e $p|b$ e $q|b$, concluímos que $n = pq|b$. Logo

$$b \equiv 0 \quad mod\ n.$$

Portanto,

$$b^{ed} \equiv 0 \quad mod\ n.$$

Segundo caso: suponhamos agora que p e q não dividem b. Pelo Teorema de Fermat temos que

$$b^{p-1} \equiv 1 \quad mod\ p$$

e

$$b^{q-1} \equiv 1 \quad mod\ q.$$

Implicando que

$$(b^{p-1})^{q-1} \equiv 1^{q-1} \quad mod\ p, \tag{3.6}$$

$$(b^{q-1})^{p-1} \equiv 1^{p-1} \quad mod\ q. \tag{3.7}$$

Das equações (3.6) e (3.7) e da Proposição 3 do apêndice Congruências, temos que

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

Assim,

$$(b^{\phi(n)})^k.b \equiv b \quad mod\ n.$$

O que equivale a

$$b \equiv D(C(b)) \quad mod\ n.$$

Terceiro caso: $p|b$ e $q \nmid b$. Do fato que $p|b$, temos que

$$b^{ed} \equiv b \quad mod\ p.$$

Como q não divide b, o pequeno teorema de Fermat implica que

$$b^{ed} \equiv b \quad mod\ q.$$

Temos que $mdc(p,q) = 1$, $p|b^{ed} - b$ e $q|b^{ed} - b$, então $n = pq|b^{ed} - b$. Então,

$$b^{ed} \equiv b \quad mod\ n.$$

Provando assim, que o bloco b é igual ao bloco decodificado $D(C(b))$.

3.1.4 Segurança do RSA

Vimos que o RSA é um método de chave pública, o que poderia levantar questionamentos sobre sua segurança. Sabemos que alguns valores, como n e e, são de conhecimento público e d de conhecimento apenas do receptor legítimo da mensagem, assim o que devemos garantir é que nenhuma pessoa consiga calcular d conhecendo apenas n e e.

Na prática só sabemos encontrar d se aplicarmos o algoritmo euclidiano estendido a $\phi(n)$ e e. Mas só sabemos calcular $\phi(n)$ se conhecemos p e q, ou seja, se fatorarmos n. Se n for grande sabemos que não existem algoritmos de fatoração eficientes.

Segundo (COUTINHO, 2009), podemos supor que alguém tenha inventado um método para calcular $\phi(n)$ a partir de n e e. Desta forma, teríamos conhecimento de $n = p.q$ e $\phi(n) = (p-1).(q-1)$. Queremos determinar p e q a partir disto. Sabemos que

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

Assim, temos que $p+q = n - \phi(n) + 1$ é conhecido. No entanto,

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

logo,

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

também é conhecido. Mas conhecendo $p+q$ e $p-q$, conseguimos calcular p e q, ou seja, fatoramos n. Portanto, não tem como descobrirmos $\phi(n)$ sem fatorarmos n.

Outra suposição seria inventar um algoritmo para calcular d diretamente. Sabemos que $ed \equiv 1 \bmod \phi(n)$, implicando no conhecimento de um múltiplo de $\phi(n)$. Novamente, teríamos a fatoração de n. A demonstração de tal afirmação pode ser encontrada em (RIVEST; SHAMIR; ADLEMAN, 1978).

3.1.5 Assinaturas

Trabalhamos até agora com a segurança da Criptografia RSA em impedir que terceiros decodifiquem uma mensagem. Mas e se um terceiro se fizer passar pelo emissor legítimo? O que nos garante que a mensagem foi realmente enviada por uma determinada pessoa sendo que a chave de codificação é de conhecimento público?

Agora, iremos tratar do problema de um "hacker" se passar pelo emissor legítimo e enviar uma mensagem enganosa. Precisamos de um garantia de quem realmente é o emissor da mensagem, precisamos que essa mensagem seja "assinada".

Vejamos como isso ocorre. Suponhamos que uma empresa queria enviar uma mensagem ao banco. Para isso, a empresa deve "assinar" essa mensagem para que o banco possa identificar

o emissor e confiar na mensagem que está recebendo. Sejam C_e e D_e as funções codificação e decodificação de um empresa e C_b e D_b as funções correspondentes do banco. As funções de codificação, tanto da empresa quanto do banco, são de conhecimento público. O que seria de costume, era a empresa usar C_b para decodificar um bloco a da mensagem e o banco usando D_b decodificaria a mensagem. Mas para garantir que foi realmente a empresa que enviou tal mensagem, para assinar a mensagem, a empresa envia para o banco $C_b(D_e(a))$. Ou seja, a empresa primeiro aplica a sua função de decodificação, que é apenas de seu conhecimento, e depois codifica o bloco da maneira usual. O banco ao receber o bloco aplica sua função D_b e em seguida aplica C_e, retornando assim a mensagem original. Isso é suficiente pois, se ao aplicar a sequencia de funções C_eD_b a mensagem fizer sentido significa que ela foi codificada usando as funções C_bD_e, implicando que a mensagem foi enviada pela empresa devido ao fato de D_e ser apenas de conhecimento da empresa. Segundo (COUTINHO, 2009), a probabilidade de uma mensagem enviada por um *hacker*, sem ter utilizado a função D_e, fazer sentido é praticamente zero.

Assim como há um constante avanço em aprimorar a segurança dos métodos de criptografia, também há um avanço nas técnicas de quebrar esses códigos. Segundo (COUTINHO, 2009), um consultor em assuntos de segurança, formado em biologia, descobriu um método para encontrar a chave de decodificação do sistema RSA levando em conta apenas o tempo que o sistema leva para confirmar a assinatura. Percebemos, desta forma, que a segurança do RSA não depende exclusivamente de algoritmos matemáticos.

3.2 Protocolo Diffie-Hellman

O maior desafio da criptografia era a troca de chaves entre correspondentes sem ser descoberta por terceiros. A comunidade dos criptologistas achavam que essa troca de chaves era impossível acontecer sem o auxilio de um intermediador. Coube a Whitfield Diffie e Martin Hellman com contribuições de Ralph Merkle, através da congruência, mostrar que, não apenas era possível, mas também era uma forma simples. Diffie e Hellman trabalharam na criptografia de chave pública enquanto Merkle trabalhou, independentemente, na distribuição de chave pública. Em 1976, Diffie e Hellman publicaram um artigo intitulado “New Directions in Cryptography” na IEEE Transactions on Information Theory, e fizeram referência ao trabalho de Merkle. Em 2016, Diffie e Hellman receberam o prêmio Turing por esse trabalho.

Vejamos a seguir a ideia da dupla americana.

Maria e José precisam trocar uma chave secreta, mas possuem apenas um meio inseguro para a troca. Então, eles escolhem dois números naturais m e a, sendo m primo e a um gerador do grupo $\mathbb{Z}_m^*$, e os tornam públicos. José escolhe outro número natural α_J e o mantém secreto. Em seguida, calcula o único número $\beta_J < m$ tal que $a^{\alpha_J} \equiv \beta_J \mod m$, e o envia para Maria. De forma análoga, Maria escolhe um número natural α_M, também secreto, e calcula o único número $\beta_M < m$ tal que $a^{\alpha_M} \equiv \beta_M \mod m$, e o envia para José. No próximo passo, José calcula $\beta_M^{\alpha_J}$, obtendo

$$\beta_M^{\alpha_J} \equiv (a^{\alpha_M})^{\alpha_J} \equiv a^{\alpha_M.\alpha_J} \equiv \alpha \mod m, \quad \text{com } \alpha < m.$$

Por sua vez, Maria calcula $\beta_J^{\alpha_M}$, obtendo

$$\beta_J^{\alpha_M} \equiv (a^{\alpha_J})^{\alpha_M} \equiv a^{\alpha_J.\alpha_M} \equiv \alpha \mod m, \quad \text{com } \alpha < m.$$

Fim do processo! Agora, Maria e José possuem a chave secreta α, que é de conhecimento apenas dos dois.

Exemplo 3.4 *Suponhamos que Maria e José tenham escolhido os números naturais $a = 30$ e $m = 239$, de conhecimento de todos. José escolhe $\alpha_J = 5$ e Maria escolhe $\alpha_M = 3$, sendo que cada um conhece apenas seu número. Vamos descobrir qual a chave secreta que ambos compartilharão.*

José faz o seguinte cálculo para encontrar β_J:

$$30^3 \equiv 232 \mod 239,$$

$$30^2 \equiv 183 \mod 239,$$

$$30^5 = 30^3.30^2 \equiv 232.183 \equiv 153 \mod 239.$$

Logo, $\beta_J = 153$.

Agora, Maria faz cálculos análogos para determinar β_M:

$$30^3 = 27000 \equiv 232 \mod 239.$$

Assim, $\beta_M = 232$.

José envia o número 153 para Maria, que, por sua vez, envia o número 232 para ele.

Para determinar a chave secreta α, José tem que reduzir 232^5 módulo 239.

$$232^2 = 53824 \equiv 49 \quad mod\ 239$$

$$232^5 = 232^2.232^2.232 \equiv 49.49.232 \equiv 162 \quad mod\ 239.$$

Portanto, $\alpha = 162$ é a chave secreta!

Agora, Maria também deve reduzir 153^3 módulo 239.

$$153^2 = 23409 \equiv 226 \quad mod\ 239$$

$$153^3 = 153^2.153 \equiv 226.153 \equiv 162 \quad mod\ 239.$$

Exatamente o que esperávamos, $\alpha = 162$.

Haveria um forma de um terceiro interceptar a mensagem e decifrá-la? Haveria como um terceiro descobrir os valores α_J e α_M que não foram divulgados?

Suponhamos que uma terceira pessoa esteja acompanhando a troca de mensagens e conhece todos os valores públicos. Essa pessoa deverá resolver as seguintes congruências para encontrar os valores que foram divulgados:

$$30^{\alpha_J} \equiv 153\ mod\ 239$$

ou

$$30^{\alpha_M} \equiv 232\ mod\ 239.$$

Resolvendo uma das congruências acima, essa pessoa também terá acesso à chave secreta α.

No exemplo que demos, os valores adotados são considerados pequenos, o que os tornam fáceis de serem descobertos. O aconselhável, para oferecer segurança, são números muito maiores, sendo m próximo de 2^{1000}. O protocolo Diffie-Hellman é suscetível a ataques do tipo "main in the middle attacks", para mais detalhes veja (AHMED et al., 2012).

3.3 Criptografia ElGmal

Taher ElGamal, nascido no Egito, vive atualmente na Califórnia e é mundialmente respeitado por suas contribuições com a criptografia. É líder de segurança da informação e reconhecido como o "pai" do SSL, protocolos criptográficos que fornecem segurança de comunicações em redes de computadores.

ElGamal criou um criptossistema que se baseia na dificuldade de calcular logaritmos discretos em $\mathbb{Z}_p^*$. Ver (ELGAMAL, 1985).

3.3.1 O Algoritmo de Criptografia ElGamal

Este algoritmo trabalha com duas chaves, uma particular e outra pública. Chamaremos os usuários de A e B.

Inicialmente, o usuário A cria uma chave particular e outra pública. Essa chave pública servirá para que o usuário B criptografe uma mensagem m e a chave particular será usada pelo usuário A para descriptografar m.

Como são criadas essas chaves?

1º) A escolhe um número primo, p.

2º) A escolhe $g \in \mathbb{Z}_p^*$, com g, preferencialmente, sendo um gerador do grupo cíclico $\mathbb{Z}_p^*$;

3º) A chave particular de A é um número $k \in \mathbb{Z}$ tal que $1 \leq k \leq p-1$;

4º) A calcula

$$r \equiv g^k \mod p. \tag{3.8}$$

Dessa forma, A cria uma chave pública (r, g, p).

Como o usuário B envia uma mensagem criptografada para A?

O usuário B usará a chave pública (r, g, p) juntamente com os seguintes passos:

1º) B escolhe um inteiro b, com $1 \leq b \leq p-2$ para ser sua chave particular e calcula

$$s \equiv g^b \mod p. \tag{3.9}$$

2º) Em seguida, para criptografar a mensagem m, B calcula:

$$\gamma \equiv m \cdot r^b \mod p. \tag{3.10}$$

3º) A mensagem criptografada é representada pelo par (s, γ).

Como o usuário A irá descriptografar a mensagem m?

Quando A recebe o par (s, γ), segue os seguintes passos para descriptografar a mensagem:

1º) A calcula, usando sua chave particular k:

$$y \equiv s^{p-1-k} \quad mod\ p. \tag{3.11}$$

2º) Em seguida, calcula:

$$m \equiv y \cdot \gamma \quad mod\ p. \tag{3.12}$$

Recuperando assim a mensagem m.

3.3.2 Exemplo numérico

Vamos mostrar como codificar e decodificar a palavra **DEUS**. Usaremos a Tabela 3.2 para a conversão das letras em números. Desta forma, a palavra **DEUS** é trocada pela sequência numérica 13143028, ou seja, o emissor deve criptografar os números 13, 14, 30 e 28.

Criptografaremos o número 13, os outros são análogos.

Primeira etapa

O usuário A escolhe um primo $p = 31$, implicando que trabalharão com o grupo $\mathbb{Z}_{31}^*$. Logo em seguida escolhe um elemento desse grupo, $g = 3$ e também sua chave particular $k = 25$.

Em seguida calcula r:

$$r \equiv 3^{25} \equiv 6 \quad mod\ 31.$$

Criando dessa forma, uma chave pública que será enviada ao usuário B: $(r, g, p) = (6, 3, 31)$.

Segunda etapa

O usuário B recebe essa chave pública e escolhe um inteiro $b = 16$ e calcula s:

$$s \equiv 3^{16} \equiv 8 \quad mod\ 31.$$

A mensagem $m = 13$ criptografada calculando-se o γ:

$$\gamma \equiv 13.6^{16} \equiv 13 \quad mod\ 31.$$

Ficando assim, a mensagem criptografada, representada pelo par $(8, 13)$.

Terceira Etapa

O usuário A recebe o par $(8, 13)$ e calcula y:

$$y \equiv 8^{31-1-25} \equiv 8^5 \equiv 1 \quad mod\ 31.$$

Logo depois, usando sua chave particular $k = 25$, descriptografa a mensagem:

$$m \equiv 1.13 \equiv 13 \quad mod\ 31.$$

Vimos então que a primeira letra da mensagem foi criptografa e descriptografada utilizando o *algoritmo de ElGamal*.

Nada impede que o usuário mande mais de uma letra por mensagem desde que m seja estritamente menor do que p.

3.3.3 Autenticidade do algoritmo

Para provar a autenticidade do algoritmo de ElGamal, precisamos mostrar que a Equação (3.12) é satisfeita. Da equação (3.11) temos que:

$$y \equiv s^{p-1-k} \quad mod\ p$$

$$y \equiv s^{p-1} \cdot s^{-k} \quad mod\ p. \tag{3.13}$$

Pelo Pequeno Teorema de Fermat, 2.10, temos que:

$$s^{p-1} \equiv 1 \quad mod\ p.$$

Assim, pela equação (3.9), podemos reescrever a equação (3.13) da seguinte forma:

$$y \equiv g^{-bk} \quad mod\ p. \tag{3.14}$$

Temos que calcular $y \cdot \gamma \ mod \ p$. Das equações (3.10) e (3.14) temos:

$$y \cdot \gamma \equiv m \cdot r^b \cdot g^{-bk} \equiv m \cdot r^b \cdot r^{-b} \equiv m \quad mod \ p$$

Provando assim que, quando a mensagem é descriptografada, retorna à mensagem original.

4 ATIVIDADES

Apresentaremos algumas sugestões de atividades para serem feitas com os alunos do Ensino Fundamental II e Médio.

4.1 $\sqrt{2}$ é um número irracional

Uma boa forma de apresentar aos alunos do Ensino Fundamental II que existem outros números além dos racionais é questioná-los sobre o valor de algumas raízes irracionais, por exemplo, $\sqrt{2}$. Aconselhamos que seja usada a calculadora para esta atividade, isso estimula o interesse dos alunos e não atrapalha o objetivo dessa atividade.

Primeiro passo

Questione-os entre quais raízes conhecidas $\sqrt{2}$ está. Como $\sqrt{2}$ é pequena, espera-se que rapidamente eles respondam entre $\sqrt{1}$ e $\sqrt{4}$.

Incentive-os a concluir que $\sqrt{2}$ deve ser um número entre 1 e 2, pois são as raízes de 1 e 4.

$$\sqrt{1} < \sqrt{2} < \sqrt{4}$$

$$1 < \sqrt{2} < 2$$

Segundo passo

Peça aos alunos que acrescentem uma casa decimal ao número 1 e verifiquem se, ao elevarem o novo número ao quadrado, ele será igual a 2.

Neste momento, indague-os sobre qual deve ser o primeiro número decimal. Como o número 2 está mais perto de 1 do que 4, assim $\sqrt{2}$ deve estar mais próxima de $\sqrt{1}$ do que de $\sqrt{4}$, ou seja, mais perto de 1 do que de 2. Isso fará com que eles escolham os números 1, 2, 3, 4 ou, no máximo, 5 para serem a primeira casa decimal.

Ao fazerem os quadrados obterão:

x	1,1	1,2	1,3	1,4	1,5
x^2	1,21	1,44	1,69	1,96	2,25

Com isso, verificarão que $1,4 < \sqrt{2} < 1,5$.

Terceiro passo

Neste momento, eles irão acrescentar a segunda casa decimal, seguindo a mesma lógica que utilizaram para a primeira. Incentive-os a perceber que 2 está apenas a 4 centésimos de distância do 1,96; enquanto 2,25 está a 25 centésimos. Assim, as tentativas serão: $1,41$; $1,42$ e $1,43$.

x	1,41	1,42	1,43
x^2	1,9881	2,0164	2,0449

Pelos resultados obtidos, espera-se que eles concluam que:

$$\sqrt{1,9881} < \sqrt{2} < \sqrt{2,0164}$$

$$1,41 < \sqrt{2} < 1,42.$$

Quarto passo

Novamente, peça que acrescentem a terceira casa decimal seguindo os critérios anteriores, esperando assim que as tentativas sejam: $1,412$; $1,413$; $1,414$ e $1,415$.

Obtendo:

x	1,412	1,413	1,414	1,415
x^2	1,993744	1,996569	1,999396	2,002225

Desta forma, concluirão que $1,414 < \sqrt{2} < 1,415$.

Após esses cálculos e observarem que os valores se aproximam de 2, os alunos costumam ficar entusiasmados e estimulados a acrescentar mais uma casa.

Quinto passo

Para finalizar os cálculos, pedimos que acrescentem a quarta casa decimal. Espera-se que as tentativas sejam: $1,4141$; $1,4142$; $1,4143$ e $1,4144$. Obtendo:

x	1,4141	1,4142	1,4143
x^2	1,99967881	1,99996164	2,00024449

Concluindo que $1,4142 < \sqrt{2} < 1,4143$.

Neste momento, o professor pode escolher acrescentar a quinta casa decimal ou já passar para a conclusão.

Conclusão

Após várias etapas, notamos que os números, ao serem elevados ao quadrado, se aproximavam cada vez mais do número dois, mas nunca são exatamente ele. Para que não haja dúvidas, peça para que os alunos façam 1,4142135623 ao quadrado e verifiquem que, mesmo com dez casas decimais, não encontramos $\sqrt{2}$. Apesar de não ser uma demonstração esse processo ilustra o fato de $\sqrt{2}$ ser irracional.

Após essa construção de raciocínio, o professor deverá apresentar a demonstração formal para seus alunos:

Demonstração: Suponhamos que $\sqrt{2}$ seja um número racional. Assim, $\sqrt{2} = \frac{p}{q}$, com p e q números inteiros sem fatores em comum, ou seja, na forma irredutível. Elevando a igualdade ao quadrado temos que:

$$2 = \frac{p^2}{q^2}$$

$$p^2 = 2 \cdot q^2 \tag{4.1}$$

Assim, temos que p^2 é um número par, consequentemente, p é par. Logo, podemos escrever $p = 2n$, com n inteiro. Substituindo $p = 2n$ na equação 4.1, temos:

$$(2n)^2 = 2 \cdot q^2 \Leftrightarrow 4n^2 = 2 \cdot q^2 \Leftrightarrow 2n^2 = q^2.$$

Novamente, temos que q^2 é um número par, logo q também é. Mas se p e q são pares, temos que $\frac{p}{q}$ não está na forma irredutível, contradizendo a hipóteses inicial. Portanto $\sqrt{2}$ é um número irracional.

■

DICA: Esta atividade também pode ser feita em um laboratório de Informática utilizando o Excel. Esse *software* auxilia nos cálculos e, diferentemente da calculadora, consegue fazer potências com mais casas decimais, facilitando a compreensão de que $\sqrt{2}$ possui infinitas casas decimais não periódicas.

4.2 Atividade 2

Propomos agora uma atividade envolvendo a criptografias RSA: **Caça ao tesouro**.

A ideia desta atividade é fazer um mapa do tesouro criptografando os números que nele aparecem. Nessa atividade, todos os grupos irão criptografar e descriptografar mensagens. A separação da quantidade de grupos e alunos fica a critério do professor.

Sugerimos que essa atividade seja realizada em quatro aulas: as duas primeiras para explicar o conteúdo, a terceira para criptografar uma mensagem e a quarta para descriptografar essa mensagem.

Suponhamos que haja 4 grupos, cada um desses grupos irá criptografar uma mensagem para o grupo “seguinte“ e descriptografar a mensagem do grupo “anterior". Por isso, já em um primeiro momento deve ficar bem clara a ordem dos grupos para que não haja erro na troca de informações. Veja a seguinte tabela:

Grupo	Criptografa para	Descriptografa de
I	II	IV
II	III	I
III	IV	II
IV	I	III

Vamos a um exemplo prático!

1ª etapa: Pré-codificação

Pegaremos o Grupo I como exemplo, os demais são análogos. Primeiramente, o Grupo I deve escolher os primos p e q para determinar $n = p \cdot q$. Em seguida devem escolher um número e de forma que $mdc(e, \phi(n)) = 1$. O último passo é determinar o inverso multiplicativo, d, de e mod $\phi(n)$. Lembrando que n e e serão de conhecimento público.

Para exemplificar, escolhemos $p = 13$, $q = 7$ e $e = 5$. Assim, encontramos $n = 91$, $\phi(91) = \phi(13 \cdot 7) = (13-1) \cdot (7-1) = 72$ e $d = 29$.

2ª etapa: Codificação

O Grupo I torna público os números n e e para que o Grupo IV criptografe uma mensagem. O Grupo IV tem a seguinte mensagem original:

"Siga 31 passos para o norte, gire 45^o para a esquerda e siga na direção oeste 61 passos.

Neste momento, os alunos deverão criptografar os número que aparecem em seu mapa. No nosso caso, devemos criptografar os números 31, 45 e 61:

$$31^5 \equiv 5 \quad mod\ 91$$

$$45^5 \equiv 54 \quad mod\ 91$$

$$61^5 \equiv 3 \quad mod\ 91$$

Portanto, a mensagem criptografada que será entregue ao Grupo I é:

"Siga 5 passos para o norte, gire 54^o para a esquerda e siga na direção oeste 3 passos".

3ª etapa: Descriptografar

O Grupo I recebe a mensagem e utilizando o número d, descriptografa a mensagem.

$$5^{29} = 5^{10+10+9} = 5^{10} \cdot 5^{10} \cdot 5^9 \equiv 51 \cdot 51 \cdot 83 \equiv 31 \quad mod\ 91$$

$$54^{29} = 54^{10+10+9} = 54^{10} \cdot 54^{10} \cdot 54^9 \equiv 23 \cdot 23 \cdot 83 \equiv 45 \quad mod\ 91$$

$$3^{29} = 3^{10+10+9} = 3^{10} \cdot 3^{10} \cdot 3^9 \equiv 81 \cdot 81 \cdot 27 \equiv 61 \quad mod\ 91$$

Note que separamos a congruência inicial em congruências menores. Como estamos trabalhando com calculadora científica, temos que nos atentar à quantidade de casas que ela consegue trabalhar, então para que não haja erros, optamos por trabalhar com essas congruências. Para o cálculo dessas congruências foi usada a calculadora científica online que pode ser encontrada em: https://www.calculadoraonline.com.br/cientifica .

Desta maneira, o Grupo I descobre que os verdadeiros valores são 31, 45 e 61. Retornando à mensagem original.

Agora, basta seguir as instruções e encontrar o "tesouro"!

O grupo campeão será aquele que gastar menor tempo para criptografar e descriptografar a mensagem. Basta somarmos o tempo gasto nas duas últimas aulas. Cabe ao professor, com criatividade, escolher qual será o “tesouro“ que os alunos encontrarão.

Ao mesmo tempo que o Grupo I estará escolhendo as chaves para o Grupo IV, os outros grupos estarão fazendo a mesmo coisa. Quando o Grupo IV tiver acesso aos valores n e e do Grupo I, o Grupo I também estará tendo acesso aos valores de n e e que o Grupo II escolheu e também terá que criptografar uma mensagem.

Sugestões:

- Escolher números primos pequenos.

- Ensinar aos alunos apenas como calcular $\phi(n)$.
- Ao invés de falar em inverso multiplicativo, explicar que para determinar o valor de d, devemos encontrar um número que multiplicado por e deixa resto 1 na divisão por $\phi(n)$. Esse inverso multiplicativo será encontrado por tentativa, mas explique que existe um algoritmo para encontrar esse inverso.

5 CONCLUSÃO

Ao longo desta dissertação observamos que os números primos são importantes não só para a Matemática, mas também para o nosso dia a dia. Com o aumento significativo do uso da tecnologia e da troca de informações pelos meios digitais fez-se necessária a criação de métodos para transmitir essas informações de forma segura. E a criptografia ajudou a tornar isso possível.

Os números primos sempre foram alvo de muitos estudos, o que nos forneceu avanços consideráveis em relação às suas propriedades e particularidades. Isso auxiliou muito no desenvolvimento da criptografia.

Com a criptografia conseguimos exemplificar a aplicação de vários conteúdos do Ensino Fundamental e Médio, tais como: divisão euclidiana, máximo divisor comum, potenciação, radiciação, propriedades transitiva, reflexiva, simétrica entre outras. O bom de ilustrar essas aplicações é que ressaltamos para os alunos a importância da Matemática em seu cotidiano.

Estudamos duas criptografias que se destacam atualmente: RSA e ElGamal. Ambas baseadas na troca de chaves assimétricas. Estudos atuais mostraram que a Criptografia ElGamal é menos arriscada que a RSA, que apresentou falta de segurança em duas de cada mil chaves coletadas. Ver (LENSTRA et al., 2012).

A criptografia foi se desenvolvendo ao longo da história e percebemos que houve muitas mudanças na forma de executá-la. O que começou apenas com uma troca na ordem das letras do alfabeto se tornou algo sofisticado e com a presença de propriedades e conceitos matemáticos mais refinados. O conhecimento não é algo estático, está sempre em movimento, e a criptografia está acompanhando esse movimento. Hoje, utilizamos os números primos na criptografia de informações e a segurança dos sistemas de criptografia baseia-se em problemas matemáticos que são difíceis de resolver nos computadores atuais. Mas vemos também um grande avanço computacional, o que poderá acarretar em uma mudança na segurança desses métodos. Pesquisas vêm sendo desenvolvidas na busca de métodos alternativos que possam substituir os que existem hoje. Estudos nos mostram que o próximo passo será a *Criptografia Quântica*, que se baseia nos princípios da mecânica quântica, não mais em números primos.

REFERÊNCIAS

AGRAWAL, M.; KAYAL, N.; SAXENA, N. Primes is in p. **Annals of Mathematics**, n. 2, p. 781–793, 2004. Disponível em: <https://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf>.

AHMED, M. et al. Diffie-hellman and its application in segurity protocols. **International Journal of Engineering Science and Innovative Technology (IJESIT)**, n. Volume 1, p. 69–73, nov 2012. Disponível em: <https://www.researchgate.net/publication/279725863>.

COUTINHO, S. C. **Primalidade em Tempo Polinomial: uma introdução ao algoritmo AKS**. 1. ed. Rio de Janeiro: Unisersidade Federal do Rio de Janeiro, 2004.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. 2. ed. Rio de Janeiro: IMPA, 2009.

COUTINHO, S. C. **Criptografia**. 1. ed. Rio de Janeiro: IMPA, 2016.

ELGAMAL, T. A public kay cryptosystem and a signatura scheme based on discrete logarithms. **IEEE Transactions on Information Theory**, n. 31, p. 469–472, 1985. Disponível em: <https://ieeexplore.ieee.org/document/1057074>. Acesso em: 04 nov. 2020.

HEFEZ, A. **Aritmética**. 2. ed. Rio de Janeiro: SBM, 2016.

KLARREICH, E. A number theorist who solves the hardest easy problems. **Quanta Magazine**, 2020. Disponível em: <https://www.quantamagazine.org/james-maynard-solves-the-hardest-easy-math-problems-20200701/>. Acesso em: 04 nov. 2020.

LENSTRA, A. et al. Ron was wrong, whit is right. **Cryptology e Print Archive**, n. 064, 2012. Disponível em: <https://eprint.iacr.org/2012/064.pdf>. Acesso em: 04 nov. 2020.

LIN, T. After prime proof, an unlikely star rises. **Quanta Magazine**, 2015. Disponível em: <https://www.quantamagazine.org/yitang-zhang-and-the-mystery-of-numbers-20150402>. Acesso em: 04 nov. 2020.

MARTINEZ, F. B.; SALDANHA, N.; TENGAN, E. **Teoria dos números**. 2. ed. Rio de Janeiro: IMPA, 2011.

MAYNARD, J. Small gaps between primes. 2019. Disponível em: <https://arxiv.org/pdf/1311.4600.pdf>. Acesso em: 04 nov. 2020.

O'CONNOR,J.J. AND ROBERTSON, E.F. **Marin Mersenne**. [S.l.], 1996. Disponível em: <https://mathshistory.st-andrews.ac.uk/Biographies/Mersenne/>. Acesso em: 04 nov. 2020.

RIBENBOIM, P. **The Little Book of Bigger Primes**. 2. ed. New York: Springer, 2004.

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. **Comm. ACM**, n. 21, p. 120–126, 1978.

SINGH, S. **O livro dos códigos**. 5. ed. Rio de Janeiro: Record, 2005.

WIKIPéDIA. **Constante de Brun — Wikipédia, a enciclopédia livre**. 2016. [Online; accessed 04-novembro-2020]. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Constante_de_Brun&oldid=47225932>.

WIKIPéDIA. **Gottfried Wilhelm Leibniz — Wikipédia, a enciclopédia livre**. 2020. [Online; accessed 4-novembro-2020]. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Gottfried_Wilhelm_Leibniz&oldid=59976305>.

WIKIPéDIA. **Último teorema de Fermat — Wikipédia, a enciclopédia livre**. 2020. [Online; accessed 20-outubro-2020]. Disponível em: <https://pt.wikipedia.org/w/index.php?title=%C3%9Altimo_teorema_de_Fermat&oldid=59631994>.

WIKIPéDIA. **Sophie Germain — Wikipédia, a enciclopédia livre**. 2020. [Online; accessed 04-novembro-2020]. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Sophie_Germain&oldid=58371821>.

ZHANG, Y. Bounded gaps between primes. **Annals of Mathematics**, n. 179, p. 1121–1174, 2014. Disponível em: <https://annals.math.princeton.edu/wp-content/uploads/annals-v179-n3-p07-s.pdf>. Acesso em: 04 nov. 2020.

APÊNDICE A – CONGRUÊNCIAS

A congruência é uma das principais ferramentas usada na criptografia, facilitando a descrição do processo de criptografia RSA e de ElGamal. O que torna a congruência extremamente útil é a sua relação com a divisão euclidiana. Apresentaremos agora alguns conceitos e teoremas que são de extrema importância para compreensão e utilização da congruência. Foi usado como referência para a elaboração desse apêndice o livro da coleção PROFMAT de Aritmética, no qual encontram-se as demonstrações aqui omitidas. Ver (HEFEZ, 2016).

Congruência

Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Escrevemos

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

Por exemplo, $34 \equiv 29 \mod 5$, pois o resto da divisão de 34 e 29 por 5 é 4, ou seja, possuem o mesmo resto.

Quando a relação $a \equiv b \mod m$ for falsa, dizemos que a e b não são congruentes módulo m e escrevemos $a \not\equiv b \mod m$.

Proposição 1 *Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, temos que*

i) $a \equiv a \mod m$;

ii) se $a \equiv b \mod m$, então $b \equiv a \mod m$;

iii) se $a \equiv b$ mod m e $b \equiv c$ mod m, então $a \equiv c$ mod m.

Proposição 2 *Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \mod m$ se, e somente se, $m|b-a$.*

Demonstração: Sejam $a = mq + r$, com $0 \leq r < m$ e $b = mt + s$, com $0 \leq s < m$, as divisões euclidianas respectivamente de a e b por m. Assim,

$$b - a = mt + s - mq - r = m(t-q) + (s-r).$$

Portanto, $a \equiv b \mod m$ se, e somente se, $r = s$, que é equivalente a dizer que $m|b-a$.

■

Temos ainda algumas propriedades adicionais:

Proposição 3 *Sejam a, b* $\in \mathbb{Z}$ *e* $m, n, m_1, m_2, ...m_r$ *inteiros maiores que 1. Temos que:*

i) se $a \equiv b$ mod m e $n|m$ então $a \equiv b$ mod n;

ii) $a \equiv b$ mod m_i, para todo $i = 1, 2, ..., r \Leftrightarrow a \equiv b$ mod $[m_1, m_2, ..., m_r]$;

Demonstração: i) Se $a \equiv b$ mod m, então $m|b-a$. Como $n|m$, temos que $n|b-a$. Logo, $a \equiv b$ mod n.

ii) ($\Rightarrow$) Se $a \equiv b$ mod m_i, com $i = 1, ..., r$, então $m_i|b-a$, para todo i. Desta forma, temos que $b-a$ é múltiplo de cada m_i. Logo, $[m_1, ..., m_r]|b-a$, implicando que $a \equiv b$ mod $mmc(m_1, ..., m_r)$. ($\Leftarrow$) Decorre do item i).

■

Da divisão euclidiana, temos que

$$a = q.m + r \text{ com } 0 \leq r < m.$$

O que equivale a dizer que

$$a \equiv r \ \ mod\ m.$$

Assim, todo inteiro positivo é congruente módulo m ao resto de sua divisão por m, que é um número entre 0 e $m-1$.

Se $a \equiv r \ \ mod\ m$ e $0 \leq r < m$, dizemos que r é o ***resíduo*** de a módulo m.

No exemplo inicial, vimos que o resto da divisão de 34 por 5 é igual a 4, então, podemos dizer que $34 \equiv 4 \ \ mod\ 5$.

Proposição 4 *Cada número tem apenas um resíduo módulo m.*

Demonstração: De fato, se

$$a \equiv r \text{ mod m, com } 0 \leq r \leq m-1 \text{ e}$$
$$a \equiv s \text{ mod m, com } 0 \leq s \leq m-1,$$

então, pela Proposição 1, temos que

$$r \equiv s\ mod\ m.$$

Sem perda de generalidade, seja $r \leq s$. Pela Preposição 2 temos que $m|s-r$, mas r e s são menores do que m, assim, $0 \leq s-r < m$. Implicando assim que $s-r$ só pode ser múltiplo de m se $s-r=0$. Portanto os resíduos r e s são iguais.

■

A proposição a seguir mostra que a congruência, que é uma relação de equivalência, é compatível com as operações de adição e multiplicação, tornando-a extremamente útil.

Proposição 5 *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.*

i) Se $a \equiv b$ mod m e $c \equiv d$ mod m, então $a+c \equiv b+d$ mod m.

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

Demonstração: Suponhamos que $a \equiv b$ mod m e $c \equiv d$ mod m. Assim, pela Proposição 2, temos que $m|b-a$ e $m|d-c$.

i) Como $m|b-a$ e $m|d-c$, temos que $m|(b-a)+(d-c)$, ou seja, $m|(b+d)-(a+c)$. Portanto, $a+c \equiv b+d$ mod m.

ii) Note que $bd-ac = bd-ad+ad-ac = d(b-a)+a(d-c)$. Como $m|b-a$ temos que $m|d(b-a)$. Da mesma forma, temos que $m|a(d-c)$. Assim, $m|d(b-a)+a(d-c)$, ou seja $m|bd-ac$. Portanto, $ac \equiv bd$ mod m.

■

Corolário 6 *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Temos que*

(i)

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

(ii)

$$a.c \equiv b.c \quad mod\ m \Leftrightarrow \quad a \equiv b \quad mod\ \frac{m}{(m,c)}.$$

Note que no item (ii) do corolário acima, se $mdc(m,c) = 1$, $a \equiv b\ mod\ m$.

Corolário 7 *Para todo $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$, se $a \equiv b\ mod\ m$, então tem-se que $a^n \equiv b^n\ mod\ m$.*

A demonstração pode ser feita por indução sobre n ou aplicando-se o segundo item da proposição anterior.

Uma outra forma de enunciar o Pequeno Teorema de Fermat usando a notação de congruência é:

Se p é um número primo e $a \in \mathbb{Z}$, então

$$a^p \equiv a \ \ mod p.$$

Mais ainda, se $p \nmid a$, então

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

Teorema de Euler

O Teorema de Euler trata-se de uma generalização do Pequeno teorema de Fermat, visto anteriormente.

Proposição 8 *Sejam $a, m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1$ mod m possui solução se, e somente se, $mdc(a,m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é um solução, então x é uma solução da congruência se, e somente se, $x \equiv x_0$ mod m.*

A demonstração dessa proposição pode ser encontrada em (HEFEZ, 2016), página 194.

Para enunciar e demonstrar o Teorema de Euler, precisamos entender o que é um *sistema completo de resíduo* e um *sistema reduzido de resíduo*.

Vimos no início do capítulo que um resíduo é o resto da divisão de um inteiro positivo por m, assim um *sistema completo de resíduo* módulo m é um conjunto de m inteiros que não são dois a dois congruentes módulo m,

Exemplo 9 *O sistema completo de resíduo módulo 5 é o conjunto $R = \{0,1,2,3,4\}$.*

Podemos notar que os elementos do conjunto R podem ser trocados por outros que deixem os mesmos restos. Como por exemplo $\{5,6,7,8,9\}$, ou ainda $\{12,13,14,15,16\}$. Percebemos que qualquer conjunto formado por 5 inteiros consecutivos é um *sistema completo de resíduo* módulo 5.

Generalizando, um conjunto de m inteiros consecutivos formam um *sistema completo de resíduos* módulo m.

Um *sistema reduzido de resíduos* módulo m é o conjunto formado por todos os elementos do sistema completo de resíduos que são primo com m.

Exemplo 10 *Seja* $R = \{0,1,2,...,19\}$ *um sistema completo de resíduos módulo 20. Agora, para acharmos um sistema reduzido de resíduos, basta retirarmos os números que não são primo com 20. Temos então que o conjunto* $R_1 = \{1,3,7,9,11,13,17,19\}$ *é um sistema reduzido de resíduos.*

Definição 11 *O número de elementos que um sistema reduzido de resíduos módulo m possui, que será denotado por* $\phi(m)$*, é chamado função fi de Euler.*

Proposição 12 *Seja* $r_1,...,r_{\phi(m)}$ *um sistema reduzido de resíduos módulo m e seja* $a \in \mathbb{Z}$ *tal que* $mdc(a,m) = 1$*. Então,* $ar_1,...,ar_{\phi(m)}$ *é um sistema reduzido de resíduos módulo m.*

Demonstração: Seja $a_1,...,a_m$ um sistema completo de resíduos módulo m do qual foi retirado o sistema reduzido de resíduos $r_1,...,r_{\phi(m)}$. Do fato de que $mdc(a,m) = 1$, tem-se que $mdc(a_i,m) = 1$ se, e somente se, $mdc(aa_i,m) = 1$, o resultado segue disso.

■

Agora, temos todos os pré-requisitos para enunciar e demonstrar o Teorema de Euler.

Teorema 13 *Sejam* $a,m \in \mathbb{Z}$*, com* $m > 1$ *e* $mdc(a,m) = 1$*. Então,*

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

Demonstração: Seja $\{r_1,r_2,...,r_{\phi(m)}\} \subset \{1,2,3,...,m-1\}$ um sistema reduzido de resíduo. Pela Preposição 12, temos que $\{ar_1,ar_2,...,ar_{\phi(m)}\}$ é outro sistema reduzido de resíduo. Desta forma, temos que cada elemento de $\{ar_1,ar_2,...,ar_{\phi(m)}\}$ é congruente a um, e apenas um, elemento de $\{r_1,r_2,...,r_{\phi(m)}\}$. Assim,

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

ou seja,

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

Como $mdc(m,r_i) = 1$, pelo Corolário 6 item (ii) , temos que

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

■

Para usarmos o Teorema de Euler, precisamos calcular $\phi(m)$, o que muitas vezes é algo extenso para se fazer usando o máximo divisor comum entre cada um dos restos com m. Desta forma, a proposição a seguir nos auxiliará no cálculo de $\phi(m)$ para um número natural m qualquer.

Proposição 14 *Se p é um número primo e r um número natural então, tem-se que*

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

Demonstração: Podemos perceber que do número 1 até p^r temos p^r números naturais. Como vimos anteriormente, para encontrarmos os elementos do sistema reduzido de resíduos, devemos retirar todos os números que não são primos com p^r, ou seja, $p, 2p, ..., p^{r-1}p$, que são ao todo p^{r-1} números. Portanto, $\phi(p^r) = p^r - p^{r-1}$.

■

Proposição 15 *Sejam $m,n \in \mathbb{N}$ tais que $mdc(m,n) = 1$. Então*

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

Demonstração: Para $m = 1$ ou $n = 1$, o resultado segue de imediato. Suponhamos que $m > 1$ e $n > 1$. Considere a seguinte tabela formada pelos números naturais de 1 a $m.n$:

1	2	...	k	...	n
n + 1	n +2	...	n +k	...	2n
...	...	...	...	...	...
(m-1).n +1	(m-1).n +2	...	(m-1).n +K	...	m.n

Temos que $mdc(t,m.n) = 1$ se, e somente se, $mdc(t,n) = mdc(t,m) = 1$. Desta forma, para calcular $\phi(m.n)$, devemos determinar quais inteiros na tabela são simultaneamente primos com m e n.

Assim, se o primeiro elemento de uma coluna não for primo com n, então todos os elementos da coluna não são primos com n. Portanto, os elementos primos com n estão necessariamente nas colunas restantes que são em número $\phi(n)$, cujos elementos são primos com n, como é fácil verificar.

Agora, veremos quais são os elementos primos com m em cada uma dessas colunas. Como $mdc(m,n) = 1$, a sequência $k,\ n+k,\ ...,(m-1).n+k$ forma um sistema completo de resíduos módulo m, pois tem m inteiros consecutivos. Assim, $\phi(m)$ desses elementos são primo com m. Portanto, o número de elementos primos com m e n, ao mesmo tempo, é $\phi(m).\phi(n)$.

■

Com as Proposições 14 e 15, podemos obter uma expressão para calcular $\phi(m)$ para qualquer $m \in \mathbb{N}$. Esse expressão é apresentada como o seguinte teorema:

Teorema 16 *Seja $m = {p_1}^{\alpha_1}...{p_n}^{\alpha_n}$, com m> 1, a decomposição de m em fatores primos. Então,*

$$\phi(m) = {p_1}^{\alpha_1-1}...{p_n}^{\alpha_n-1}.(p_1-1)...(p_n-1).$$

A demonstração desse teorema segue direto das proposições citadas acima.

Exemplo 17 Calcular $\phi(20)$ pela expressão do teorema anterior.

Temos que

$$\phi(20) = \phi(2^2.5) = 2^1.5^0.(2-1).(5-1) = 2.1.1.4 = 8.$$

Exatamente como havíamos encontrado no Exemplo 10.

Inversos modulares

Observe as seguintes congruências.

$$3.5 \equiv 1\ mod\ 7$$

$$4.7 \equiv 1\ mod\ 9$$

Se utilizarmos a linguagem que usamos com os racionais, podemos dizer que 1 "dividido" por 3 módulo 7 tem como resultado o 5. O mesmo vale para a segunda congruência, 1 "dividido" por 4 módulo 9, tem como resultado o número 7. Quando isso ocorre, dizemos que 3 e 5 são inversos módulo 7 e, no segundo caso, 4 e 7 são inversos módulo 9.

Sistematizando, a e a' são inversos módulo n se

$$a.a' \equiv 1\ mod\ n.$$

Da mesma forma que a é inverso de a', temos também que a' é inverso de a.

Note que 0 não possui inverso para nenhum n, visto que $0.a \equiv 0\ mod\ n$, sendo a um inteiro qualquer.

Será que, com exceção do 0, todo os números de 1 a $n-1$ possuem inverso módulo n?

Abaixo encontramos os inverso dos números módulo 7 e os inversos módulo 10.

	Inverso módulo 7
1	1
2	4
3	5
4	2
5	3
6	6

Tabela 1 – Tabela dos inversos módulo 7

	Inverso módulo 10
1	1
2	-
3	7
4	-
5	-
6	-
7	3
8	-
9	9

Tabela 2 – Tabela dos inversos módulo 10

Os inversos nas tabelas foram determinados por tentativa. Ou seja, para acharmos o inverso de 2 módulo 7, multiplicamos 2 pelos inteiros 2, 3 e 4, até que encontramos seu inverso, o 4. O mesmo fizemos com o 3, encontrando o 5. Para o número 4 e o 5 não foram necessárias contas visto que eles já eram inversos do 2 e 3 respectivamente, desta forma o inverso do 4 é o 2 e o inverso do 5 é o 3. Faltando assim apenas o 6, cujo inverso é ele mesmo.

Note que os inversos também estão entre 1 e $n-1$, pois todo inteiro é congruente módulo n ao seu resíduo. Note ainda que cada inteiro entre 1 e $n-1$ possui exatamente um inverso nesse intervalo. A prova de tal afirmação pode ser encontrada em (COUTINHO, 2016).

De forma análoga, fizemos a tabela de inversos módulo 10. No entanto, verificamos que alguns números não possuíam inversos.

O que nos retorna à pergunta inicial com uma reposta negativa e nos dá o seguinte teorema:

Teorema 18 *Dado $a \in \mathbb{Z}$, temos que a possui inverso módulo m se, e somente se, $mdc(a,m) = 1$.*

A demonstração desse teorema segue direto da Proposição 8.

APÊNDICE B – LOGARITMO DISCRETO

Neste apêndice abordaremos alguns tópicos que serão necessários para compreensão da Criptografia ElGamal. Trabalharemos com Grupos e Logaritmos discretos.

Grupos

Um grupo é constituído por dois ingredientes básicos: um conjunto e uma operação fechada definida neste conjunto. Digamos que o conjunto seja G e a operação seja $\cdot$. Por operação fechada entendemos uma regra que a cada dois elementos $a, b \in G$ associa um terceiro elemento $a \cdot b$ que também está em G. Além do conjunto e da operação fechada, precisamos que algumas condições sejam satisfeitas, como segue na definição:

Definição 1 *Um conjunto G com uma operação*

$$G \times G \to G$$
$$(a,b) \rightarrowtail a \cdot b$$

é um grupo se as seguintes condições são satisfeitas:

i) A operação é associativa, isto é

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \text{ para todo } a,b,c \in G$$

ii) Existe um elemento neutro, isto é, existe $e \in G$ tal que

$$a \cdot e = e \cdot a = a.$$

iii) Todo elemento possui um elemento inverso, isto é, para todo $a \in G$, existe $b \in G$ tal que

$$a \cdot b = b \cdot a = e.$$

Vamos demonstrar agora que, tanto o elemento neutro, quando o elemento inverso, são únicos.

Teorema 2 *O elemento neutro é único.*

Demonstração: Suponha que existam $e, e' \in G$ tais que ambos sejam elementos neutros de G. Como e é um elemento neutro de G, temos que

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

Por outro lado, e' também é elemento neutro de G, então

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

Assim,

$$e = e'.$$

Portanto o elemento neutro é único.

■

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

Demonstração: Suponhamos que existam $b, c \in G$ tais que ambos são elementos inversos de $a \in G$. Usando as propriedades de grupo, temos:

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

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

■

Exemplo 4 *Sejam $n > 1$ um inteiro e $\bar{r} = \{kn + r \,|k \in \mathbb{Z},\ 0 \leq r < n\}$. Considere o conjunto*

$$\mathbb{Z}_n = \{\overline{1}, \overline{2}, ..., \overline{n-1}\},$$

e definindo a operação de adição sobre $\mathbb{Z}_n$ como sendo

$$\overline{x} + \overline{y} = \overline{x+y} = \overline{s},$$

sendo s o resto da divisão de $\overline{x+y}$ por n, temos que $(\mathbb{Z}_n, +)$ é um grupo.

Exemplo 5 *Seja n primo. Considerando o conjunto*

$$\mathbb{Z}_n^* = \{\overline{1}, \overline{2}, ..., \overline{n-1}\}$$

e definindo a operação de multiplicação sobre $\mathbb{Z}_n$ como sendo

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y} = \overline{s},$$

sendo s o resto da divisão de $\overline{x \cdot y}$ por n, temos que $(\mathbb{Z}_n, \cdot)$ é um grupo.

Definição 6 *Seja G um conjunto munido com uma operação binária $(a,b) \rightarrowtail a.b$ que satisfaz as seguintes condições:*

i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in G$

ii) Existe elemento neutro $1 \in G$ tal que

$$a \cdot 1 = 1 \cdot a = a.$$

iii) Todo elemento possui um elemento inverso, isto é, para todo $a \in G$, existe $b \in G$ tal que

$$a \cdot b = b \cdot a = 1.$$

Então, dizemos que $(G, .)$ é um grupo multiplicativo.

Subgrupos

Dado um grupo G, vamos estudar seus subconjuntos que com a operação herdada de G também satisfazem as condições requeridas para ser um grupo. Esse subconjuntos são chamados de subgrupo de G.

Definição 7 *Seja $(G, \cdot)$ um grupo. Um subconjunto não vazio H de G é um subgrupo de G quando, com a operação de G, o conjunto H é um grupo, isto é, quando as seguinte condições são satisfeitas:*

i) $h_1 \cdot h_2 \in H$, *para todo* $h_1, h_2 \in H$;

ii) $h_1 \cdot (h_2 \cdot h_3) = (h_1 \cdot h_2) \cdot h_3$, *para todo* $h_1, h_2, h_3 \in H$;

iii) Existe $e \in H$ tal que $e \cdot h = h \cdot e = h$, *para todo* $h \in H$;

iv) para cada $h \in H$ *existe* $h^{-1} \in H$ tal que $h \cdot h^{-1} = h^{-1} \cdot h = e$.

A primeira condição serve para que a operação $(\cdot)$ esteja bem definida em H, as demais decorrem do fato de H ser grupo.

Definição 8 *Dado a um elemento do grupo G, denotamos por $< a >$ o conjunto de todas as potências de a, ou seja,*

$$< a > = \{a^n : n \in \mathbb{Z}\},$$

sendo $a^n = \underbrace{a.a.\ \ldots\ .a}_{n\ vezes}$, *quando* $n > 0$, $a^n = \underbrace{a^{-1}.a^{-1}.\ \ldots\ .a^{-1}}_{n\ vezes}$, *quando* $n < 0$ *e* $a^0 = e$, *sendo e o elemento neutro da operação do grupo.*

A definição acima faz com que $< a >$ seja um subgrupo de G, algo que é facilmente verificável.

Definição 9 *O conjunto* $< a >$ *é o subgrupo gerado por a. Chamamos a de gerador de* $< a >$.

Com isso, podemos definir grupos que podem ser gerados por um elemento.

Definição 10 *Um grupo G é cíclico quando ele pode ser gerado por um elemento de G, ou seja, existe* $g \in G$ *tal que* $G =< g >$.

O problema do Logaritmo Discreto

Começaremos relembrando a definição de logaritmo real. Dados dois números reais positivos, a e b, com $a > 0$ e $a \neq 1$, devemos encontrar o único número real x, tal que

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

O *logaritmo discreto* possui uma definição análoga, porém necessitamos da congruência módulo n.

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

$$\alpha^x = \beta.$$

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

Seja a um gerador de $\mathbb{Z}_p^*$, p primo, e seja b um elemento não nulo de $\mathbb{Z}_p^*$. O *Problema do Logaritmo Discreto* consiste em encontrar um expoente x inteiro tal que,

$$a^x \equiv b \mod p.$$

Proposição 11 *Se existir* $x \in \mathbb{Z}$ *tal que* $a^x \equiv b \mod p$, *então esta congruência possui infinitas soluções em* $\mathbb{Z}$.

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

Proposição 12 *Dado um inteiro fixo* $a \neq 0$, *o problema do logaritmo discreto* $a^x \equiv b \mod p$ *possui solução em* $\mathbb{Z}_p$ *para qualquer* $b \in \mathbb{Z}_p$ *com* $b \not\equiv 0 \mod p$ *se, e somente se, a é um gerador do grupo multiplicativo* $\mathbb{Z}_p^*$.

Demonstração: Considere que $a^x \equiv b \ mod\ p$ possui solução em $\mathbb{Z}_p$ para todo inteiro b. Ou seja, qualquer que seja $b \in \mathbb{Z}_p$, existe um $x \in \mathbb{Z}_p$ tal que $a^x \equiv b \ mod\ p$. Assim, a é gerador de $\mathbb{Z}_p^*$.

Agora, seja a um gerador de $\mathbb{Z}_p^*$. Temos que cada elemento de $\mathbb{Z}_p$ é congruente a alguma potência de a. Portanto, para todo $b \in \mathbb{Z}_p$, existe $x \in \mathbb{Z}_p$ tal que $a^x \equiv b \ mod\ p$. Provando assim que o problema do logaritmo discreto possui solução.

■

Exemplo 13 *Calcular* $x = \log_3 4$ *em* $\mathbb{Z}_5$

Primeiro devemos verificar que 3 *é um gerador do grupo multiplicativo* $\mathbb{Z}_5^*$. *De fato, pois todos os elementos de* $\mathbb{Z}_5{}^*$ *são gerados por uma potência de* 3*:*

$3^0 = 1$	$3^1 = 3$	$3^2 = 4$	$3^3 = 2$	$3^4 = 1$

Logo, pela proposição anterior, sabemos que o logaritmo possui solução. Temos que:

$$x = \log_3 4 \Leftrightarrow 3^x \equiv 4 \ mod\ 5,$$

o que ocorre quando $x = 2$.

O exemplo dado é de fácil execução, porém, quando escolhemos convenientemente p e a, principalmente p grande, a resolução torna-se mais difícil. Parte da segurança do Protocolo Diffie-Hellman é baseada nesse fato.