RMAT
ISSN: 2237-8103
REVISTA DE MATEMÁTICA DA UFOP

OPEN ACCESS
Volume 1, Número 1, 2025
10.63801/rmat.v1i.7871
Recebido: 26/02/2025
Publicado: 08/10/2025

Testes Determinísticos de Primalidade

Deterministic Primality Tests
Pruebas Determinísticas de Primalidad

Daniel Valadares
<daniel.valadares@aluno.ufop.edu.br>
Universidade Federal de Ouro Preto, Ouro Preto, MG, Brasil

Sávio Ribas
<savio.ribas@ufop.edu.br>
Universidade Federal de Ouro Preto, Ouro Preto, MG, Brasil
<https://orcid.org/0000-0002-8632-4764>

Resumo
Neste trabalho, apresentamos alguns dos testes determinísticos de primalidade mais utilizados atualmente. O objetivo é determinar, de forma computacionalmente eficiente, se um número n grande é primo, utilizando diversos resultados da Teoria dos Números. Embora essa questão tenha sido considerada puramente teórica por muito tempo, ela se tornou crucial para problemas práticos, especialmente na área da criptografia. Os testes mais comuns baseiam-se no Pequeno Teorema de Fermat e são especialmente aplicáveis a números de determinadas formas, como os números de Fermat, Fermat generalizados, Proth e Mersenne. Também introduziremos o famoso teste AKS. Vamos demonstrar e discutir cada um dos testes.

Palavras-chave: *Números primos. Testes de primalidade. Testes determinísticos.*

Abstract
In this paper, we present some of the most widely used deterministic primality tests today. The goal is to determine, in a computationally efficient way, whether a large number n is prime, using several results from Number Theory. Although this question was considered purely theoretical for a long time, it has become crucial for practical problems, especially in the area of cryptography. The most common tests are based on Fermat's Little Theorem and are especially applicable to numbers of certain shapes, such as Fermat, generalized Fermat, Proth and Mersenne numbers. We will also introduce the famous AKS test. We will demonstrate and discuss each of the tests.

Keywords: *Prime numbers. Primality tests. Deterministic tests.*

Resumen
En este trabajo presentamos algunas de las pruebas determinísticas de primalidad más utilizadas en la actualidad. El objetivo es determinar, de forma computacionalmente eficiente, si un número grande n es primo, utilizando varios resultados de la teoría de números. Aunque durante mucho tiempo esta cuestión se consideró puramente teórica, la misma se ha vuelto crucial para problemas prácticos, especialmente en el área de la criptografía. Las pruebas más comunes se basan en el pequeño teorema de Fermat y son especialmente aplicables a números de ciertas formas, como Fermat, Fermat generalizado, Proth y números de Mersenne. También presentaremos la famosa prueba AKS. Demostraremos y discutiremos cada una de las pruebas.

Palabras-Clave: *Números primos. Pruebas de primalidad. Pruebas deterministas.*

1. INTRODUÇÃO

Desde a Grécia Antiga já é conhecido que existem infinitos números primos (uma demonstração pode ser encontrada em (Ribenboim, 2014)). Um problema que se decorre naturalmente disso é o de determinar se um certo número n (grande) é ou não primo. Apesar de ter sido por muito tempo só um problema teórico de Teoria dos Números, hoje em dia esta se tornou uma questão crucial para problemas práticos, por exemplo em questões de criptografia (mais sobre isso pode ser encontrado em (Coutinho, 2014)).

Um primeiro teste seria verificar se n é divisível por cada primo menor do que ele: em caso negativo, ele é primo. Uma ideia um pouco melhor é usar o Crivo de Eratóstenes, que reduz a lista de possíveis fatores de n a serem testados apenas para os primos $p \leqslant \sqrt{n}$. Infelizmente esse teste ainda é muito lento para números grandes. Para se testar a primalidade de um número de 100 algarismos, por exemplo, seria necessário testar a divisibilidade por cada primo de até 50 algarismos, o que torna o processo computacionalmente inviável.

Durante os últimos séculos, muitos outros algoritmos, crivos e testes foram estudados pelos matemáticos, podendo os testes de primalidade ser divididos em dois tipos: determinísticos e probabilísticos. O primeiro tipo retorna o resultado "n é composto" ou "n é primo", como o Crivo de Eratóstenes, enquanto o segundo retorna que "n é composto" ou "n provavelmente é primo" (mais detalhes sobre o assunto podem ser encontrados em (Martinez *et al.*, 2024)). Quando se tem uma lista de números para testar a primalidade, é comum usar um teste probabilístico como primeiro filtro (por serem mais rápidos) e, só então, aplicar um teste determinístico aos que restaram.

Neste trabalho, olhando pelo ponto de vista de um matemático, iremos nos ater aos testes determinísticos, que trazem uma certeza em relação à primalidade do número. Para certas classes de números, alguns testes são mais eficientes do que outros. Por exemplo, se a fatoração de $n-1$ for conhecida (como nos números de Fermat), então poderemos aplicar facilmente os testes da Seção 3. Exibiremos, na Seção 4, um teste eficaz para números da forma $2^n - 1$. Por fim, na Seção 5, trabalharemos com o famoso teste AKS.

2. PRELIMINARES

Antes de trabalharmos propriamente com alguns testes determinísticos, é necessário apresentar alguns conceitos e resultados preliminares que serão usados neste artigo. Os resultados desta seção terão as demonstrações omitidas, mas estas podem ser encontradas em qualquer livro de Teoria dos Números, como (Martinez *et al.*, 2024).

Definição 1. *A* função totiente, *ou* função phi de Euler, *é definida como* $\varphi : \mathbb{N} \to \mathbb{N}$ *dada por* $\varphi(n) = \#\{m \in \mathbb{N};\ m \leqslant n \text{ e } \mathrm{mdc}(m,n) = 1\}$.

Proposição 2. *Sejam* p *um número primo e* $k \in \mathbb{N}$. *Então* $\varphi(p^k) = p^k - p^{k-1}$.
Em particular, $n \in \mathbb{N}$ *é primo se, e somente se,* $\varphi(n) = n - 1$.

Proposição 3. *Sejam* $m, n \in \mathbb{N}$ *com* $\mathrm{mdc}(m,n) = 1$. *Então* $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.
Em particular, vale $\varphi(n) < n$ *para todo* $n > 1$.

Teorema 4 (Euler-Fermat). *Sejam* $a, n \in \mathbb{N}$ *com* $\mathrm{mdc}(a,n) = 1$. *Então* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Teorema 5 (Pequeno Teorema de Fermat). *Sejam* p *primo e* $a \in \mathbb{N}$. *Então* $a^p \equiv a \pmod{n}$.

Definição 6. *A* ordem de a módulo n, *denotada por* $\mathrm{ord}_n(a)$, *em que* $a, n \in \mathbb{N}$ *são primos entre si, é definida como* $\mathrm{ord}_n(a) = \min\{t \in \mathbb{N};\ a^t \equiv 1 \pmod{n}\}$.

Proposição 7. *Sejam* $a, n, t \in \mathbb{N}$. *Então* $a^t \equiv 1 \pmod{n}$ *se, e somente se,* $\mathrm{ord}_n(a) \mid t$.
Em particular, $\mathrm{ord}_n(a) \mid \varphi(n)$.

Definição 8. *Sejam* $p > 2$ *um número primo e* $x, d \in \mathbb{Z}$. *Dizemos que* d *é um* resto quadrático módulo p *se a equação* $x^2 \equiv d \pmod{p}$ *possuir solução.*

Definição 9. *Sejam* $p > 2$ *um número primo e* $a \in \mathbb{Z}$. *Definimos o* símbolo de Legendre *como:*

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \text{se } p \nmid a \text{ e } a \text{ não é um resto quadrático módulo } p, \\ +1, & \text{se } p \nmid a \text{ e } a \text{ é um resto quadrático módulo } p, \\ 0, & \text{se } p \mid a. \end{cases}$$

Teorema 10 (Critério de Euler). *Sejam* $a \in \mathbb{Z}$ *e* $p > 2$ *primo. Então* $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Proposição 11. *O* símbolo de Legendre *possui as propriedades abaixo:*

i) *Se* $a \equiv b \pmod{p}$, *então* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

ii) *Se* $p \nmid a$, *então* $\left(\frac{a^2}{p}\right) = 1$;

iii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. *Assim,* -1 *é resto quadrático módulo* $p \iff p \equiv 1 \pmod{4}$;

iv) $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Teorema 12 (Reciprocidade Quadrática).

i) *Sejam* p *e* q *primos ímpares distintos. Então,* $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

ii) *Seja* p *um primo ímpar. Então,* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{se } p \equiv \pm 1 \pmod{8}, \\ -1, & \text{se } p \equiv \pm 3 \pmod{8}. \end{cases}$

Além desses resultados, usaremos também neste artigo alguns conceitos básicos de Álgebra, que podem ser encontrados em livros como (Gonçalvez, 2009) e (Lidl; Niederreiter, 1997). Iremos pressupor ainda que o leitor conhece as definições de grupo (multiplicativo), anel e corpo.

Denotaremos o quociente $\mathbb{Z}/p\mathbb{Z}$ por $\mathbb{Z}_p$. Temos que $\mathbb{Z}_p$ é um corpo se, se somente se, p for primo. Definimos o anel $\mathbb{Z}_p[x] = \{a_0 + a_1 x + \ldots + a_n x^n; n \in \mathbb{N}$ e $a_i \in \mathbb{Z}_p$, para $0 \leqslant i \leqslant n\}$. Se $f(x) \in \mathbb{Z}_p[x]$, então o máximo de raízes que $f(x)$ pode ter é $\partial f(x)$, o *grau do polinômio*

$f(x)$, e definimos também o anel quociente $\mathbb{Z}_p[x]/\langle f(x)\rangle$. Temos que o anel $\mathbb{Z}_p[x]/\langle f(x)\rangle$ é um corpo se, e somente se, $f(x)$ for irredutível e, nesse caso, terá $p^{\partial f(x)}$ elementos. Além disso, $\mathbb{Z}_p[x]/\langle f(x)\rangle$ é o único corpo com $p^{\partial f(x)}$ elementos (a menos de isomorfismos).

Seja G um grupo multiplicativo. Dizemos que $h_1, h_2, \ldots, h_n$ *geram* G se todo $g \in G$ puder ser escrito como $g = h_1^{\alpha_1} \cdot h_2^{\alpha_2} \cdot \ldots \cdot h_n^{\alpha_n}$, com $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}$, e denotamos por $G = \langle h_1, h_2, \ldots, h_n\rangle$. A *ordem de um grupo* G, denotada por $|G|$, é o seu número de elementos. Por exemplo, a ordem do grupo multiplicativo $\mathbb{Z}_n^\times$ é $\left|\mathbb{Z}_n^\times\right| = \varphi(n)$. Se $H \subset G$ é um grupo com a mesma operação de G, então H *é um subgrupo de* G e podemos utilizar o seguinte resultado:

Teorema 13 (Lagrange)**.** *Se H é um subgrupo de G, então $|H|$ divide $|G|$.*

3. TESTES BASEADOS NA FATORAÇÃO DE $n-1$

Nesta seção, iremos apresentar um teste determinístico para testar a primalidade de números n tais que a fatoração de $n-1$ é conhecida. Antes, é necessário vermos o seguinte resultado auxiliar:

Lema 14. *Seja $n-1 = m \cdot p^k$, com p primo e $\mathrm{mdc}(m,p) = 1$. Se existe algum $a \in \mathbb{N}$ tal que $a^{n-1} \equiv 1 \pmod n$ e $a^{(n-1)/p} \not\equiv 1 \pmod n$, então $p^k \mid \mathrm{ord}_n(a)$.*

Demonstração. Por hipótese, temos que:

$$a^{n-1} \equiv 1 \pmod n \iff a^{m\cdot p^k} \equiv 1 \pmod n, \tag{1}$$

$$a^{(n-1)/p} \not\equiv 1 \pmod n \iff a^{m\cdot p^{k-1}} \not\equiv 1 \pmod n. \tag{2}$$

Seja $d = \mathrm{mdc}(m, \mathrm{ord}_n(a))$. Então temos que $a^{m\cdot p^k} = a^{q\cdot d\cdot p^k}$ para algum $q \in \mathbb{N}$. Daí, pela congruência (1), temos que $a^{q\cdot d\cdot p^k} \equiv 1 \pmod n$; o que nos garante, pela Proposição 7, que $\mathrm{ord}_n(a) \mid q \cdot d \cdot p^k$. Como $\mathrm{mdc}(q, \mathrm{ord}_n(a)) = 1$, obtemos $\mathrm{ord}_n(a) \mid d \cdot p^k$. E como $d \mid \mathrm{ord}_n(a)$, obtemos $\dfrac{\mathrm{ord}_n(a)}{d} \mid p^k$. Por p ser primo e $\dfrac{\mathrm{ord}_n(a)}{d} \mid p^k$, segue que $\mathrm{ord}_n(a) = d \cdot p^j$ para algum $j \in \{1, 2, \ldots, k-1, k\}$.

Suponha por absurdo que $j \in \{1, 2, \ldots, k-1\}$: temos que $k - j - 1 \geqslant 0$ e $a^{\mathrm{ord}_n(a)} = a^{d\cdot p^j}$, então $a^{d\cdot p^j} \equiv 1 \pmod n$ pela Definição 6. Elevando ambos os lados da equivalência por $q \cdot p^{k-j-1}$, temos que $a^{q\cdot d\cdot p^{j+(k-j-1)}} = a^{m\cdot p^{k-1}} \equiv 1 \pmod n$, o que é um absurdo, pois contradiz a nossa hipótese (2). Portanto, $j = k$. Assim, $\mathrm{ord}_n(a) = d \cdot p^k$, isto é, $p^k \mid \mathrm{ord}_n(a)$. $Q.E.D.$

A seguir, exibiremos o primeiro teste baseado na fatoração de $n-1$ e uma aplicação.

Teorema 15. *Se para cada fator primo p de $n-1 > 0$ existe $a \in \mathbb{N}$ tal que $a^{n-1} \equiv 1 \pmod n$ e $a^{(n-1)/p} \not\equiv 1 \pmod n$, então n é primo.*

Demonstração. Sejam p um divisor primo de $n-1$ e $k, m \in \mathbb{N}$ tais que $n - 1 = m \cdot p^k$, com $\mathrm{mdc}(p, m) = 1$. Pelo lema anterior, temos que $p^k \mid \mathrm{ord}_n a$. Como $\mathrm{ord}_n(a) \mid \varphi(n)$ pela Proposição 7, então $p^k \mid \varphi(n)$ para cada fator primo de $n-1$, ou seja, $n-1 \mid \varphi(n)$, o que implica que $n - 1 \leqslant \varphi(n)$, e $\varphi(n) < n$ pela Proposição 3. Portanto, $\varphi(n) = n - 1$ e, pela Proposição 2, temos que n é primo. $Q.E.D.$

Exemplo 16. *Verificaremos se* $n = 61\,001$ *é primo. Note que* $n - 1 = 61\,000 = 2^3 \cdot 5^3 \cdot 61$. *Para provar que* n *é primo, precisamos encontrar* a_2, a_5 *e* a_{61} *tais que* $a_p^{n-1} \equiv 1 \pmod{n}$ *e* $a_p^{(n-1)/p} \not\equiv 1 \pmod{n}$, *com* $p \in \{2, 5, 61\}$:

- $a_2 = 3 \implies 3^{61\,000} \equiv 1 \pmod{61\,001}$ *e* $3^{30\,500} \equiv -1 \neq 1 \pmod{61\,001}$;
- $a_5 = 3 \implies 3^{61\,000} \equiv 1 \pmod{61\,001}$ *e* $3^{12\,200} \equiv 21\,868 \neq 1 \pmod{61\,001}$;
- $a_{61} = 2 \implies 2^{61\,000} \equiv 1 \pmod{61\,001}$ *e* $2^{1\,000} \equiv 23\,624 \neq 1 \pmod{61\,001}$.

Portanto, pelo Teorema 15, $n = 61\,001$ *é um número primo.*

O seguinte critério, conhecido como critério de Pocklington determina a forma dos possíveis fatores primos de n.

Proposição 17 (Critério de Pocklington). *Seja* $n - 1 = m \cdot p^k$, *com* p *primo e* $\mathrm{mdc}(m, p) = 1$. *Se existe* $a \in \mathbb{N}$ *tal que* $a^{n-1} \equiv 1 \pmod{n}$ *e* $\mathrm{mdc}(a^{(n-1)/p} - 1, n) = 1$, *então qualquer fator primo* q *de* n *é tal que* $q \equiv 1 \pmod{p^k}$.

Demonstração. Como $q \mid n$, concluímos da hipótese $a^{n-1} \equiv 1 \pmod{n}$ que $n \mid a^{n-1} - 1$ e, portanto, $q \mid a^{n-1} - 1$, ou seja, $a^{n-1} \equiv 1 \pmod{q}$. Concluímos também, da hipótese $\mathrm{mdc}(a^{(n-1)/p} - 1, n) = 1$, que $q \nmid a^{(n-1)/p} - 1$, o que equivale a $a^{(n-1)/p} \not\equiv 1 \pmod{q}$. Portanto, $a^{n-1} \equiv 1 \pmod{q}$ e $a^{(n-1)/p} \not\equiv 1 \pmod{q}$. Aplicando o Lema 14, temos que $p^k \mid \mathrm{ord}_q(a)$. Pela Proposição 7, temos que $\mathrm{ord}_q(a) \mid \varphi(q)$ e, pela Proposição 2, $\varphi(q) = q - 1$, o que nos leva a $\mathrm{ord}_q(a) \mid q - 1$. Portanto, $p^k \mid q - 1$, isto é, $q \equiv 1 \pmod{p^k}$. $Q.E.D.$

O próximo teorema, conhecido como teste de Pocklington-Lehmer, nos permite testar a primalidade de n sem precisar conhecer sua fatoração completa.

Teorema 18 (Teste de Pocklington-Lehmer). *Seja* $n - 1 = m \cdot \ell$, *com* $m > \sqrt{n}$ *e* $\mathrm{mdc}(m, \ell) = 1$. *Se para cada fator primo* p *de* m *existe* $a \in \mathbb{N}$ *tal que* $a^{n-1} \equiv 1 \pmod{n}$ *e* $\mathrm{mdc}(a^{(n-1)/p} - 1, n) = 1$, *então* n *é primo.*

Demonstração. Seja $m = d \cdot p^k$, com $k \in \mathbb{N}$ e $\mathrm{mdc}(d, p) = 1$. Então $n - 1 = (d \cdot \ell) \cdot p^k$ e $\mathrm{mdc}(d \cdot \ell, p) = 1$. Pela proposição anterior, todo fator primo q de n é tal que $q \equiv 1 \pmod{p^k}$. Como essa congruência é válida para todo fator primo p de m, então qualquer fator primo q de n é tal que $q \equiv 1 \pmod{m}$. Portanto, $m \mid q - 1$, o que nos garante que $q - 1 \geqslant m$. Como $m > \sqrt{n}$ por hipótese, então $q - 1 > \sqrt{n}$, ou ainda, $q > \sqrt{n}$.

Suponha por absurdo que n não seja um número primo: há então pelo menos dois fatores primos q_1 e q_2 de n e ambos são maiores do que $\sqrt{n}$, logo $q_1 \cdot q_2 > \sqrt{n} \cdot \sqrt{n} = n$, ou seja, $q_1 \cdot q_2 \mid n$ e $q_1 \cdot q_2 > n$, o que é um absurdo. Portanto, n é primo. $Q.E.D.$

Exemplo 19. *Vamos verificar se* $27\,457$ *é um número primo. Se* $n = 27\,457$, *então* $n - 1 = 27\,456 = 2^6 \cdot 3 \cdot 143$. *Como* $2^6 \cdot 3 > 143$, *certamente* $2^6 \cdot 3 > \sqrt{n}$ *e temos que* $\mathrm{mdc}(2^6 \cdot 3, 143) = 1$, *o que nos permite usar o teorema anterior para testar a primalidade de* $27\,457$. *Para isso, devemos buscar um* $a_p \in \mathbb{N}$ *para cada* $p \in \{2, 3\}$ *tal que* $a_p^{27\,456} \equiv 1 \pmod{27\,457}$ *e* $\mathrm{mdc}(a_p^{27\,456/p} - 1, 27\,457) = 1$:

- $a_2 = 5 \implies 5^{27\,456} \equiv 1 \pmod{27\,457}$ *e* $\mathrm{mdc}(5^{13\,728} - 1, 27\,457) = 1$;
- $a_3 = 3 \implies 3^{27\,456} \equiv 1 \pmod{27\,457}$ *e* $\mathrm{mdc}(3^{9\,152} - 1, 27\,457) = 1$.

Portanto, pelo Teorema 18, $n = 27\,457$ é um número primo.

Há algumas classes de números n, mesmo que muito grandes, cuja fatoração de $n-1$ é facilmente encontrada. Alguns exemplos são os números de Fermat, de Fermat generalizado e de Proth, que definiremos a seguir:

Definição 20. *Um* número de Fermat *é um número da forma $F_n = 2^{2^n} + 1$. Um* número de Fermat generalizado *é um número da forma $a^{2^n} + 1$.*

Proposição 21. *Sejam $a, m \geqslant 2$ inteiros. Se $a^m + 1$ é primo, então a é par e m é potência de 2.*

Demonstração. Se a fosse ímpar, então $a^m + 1 > 2$ seria par, o que é um absurdo. Se m não é potência de 2, então possui um divisor ímpar $t > 1$ tal que $m = k \cdot t$ para algum $k \in \mathbb{N}$. Assim, temos $a^m + 1 = (a^k)^t + 1 \equiv (-1)^t + 1 \equiv 0 \pmod{a^k + 1}$, o que significa que $a^m + 1$ não é primo, outro absurdo. $Q.E.D.$

Definição 22. *Um* número de Proth *é um número da forma $h \cdot 2^n + 1$, onde $h < 2^n$ é ímpar.*

Primos de Fermat, de Fermat generalizado e de Proth são números de Fermat, de Fermat generalizado e de Proth que são primos, respectivamente. Dos 20 maiores primos conhecidos atualmente, 2 são de Fermat generalizados e 2 são de Proth.

Ainda hoje são conhecidos apenas 5 primos de Fermat ($F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65\,537$), sendo ainda um problema em aberto determinar se existem outros. O seguinte teste determinístico se aplica aos números de Fermat:

Teorema 23 (Teste de Pépin)**.** *Seja $n \geq 1$ um inteiro. Então $F_n = 2^{2^n} + 1$ é primo se, e somente se, $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.*

Demonstração. Se F_n é primo, então pelo Critério de Euler (10) e pelo Teorema 12 temos que $3^{(F_n-1)/2} \equiv \left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1 \pmod{F_n}$. Se $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, então $3^{(F_n-1)/2} \not\equiv 1 \pmod{F_n}$ e $3^{F_n-1} \equiv 1 \pmod{F_n}$. Logo, pelo Teorema 15, F_n é primo. $Q.E.D.$

Exemplo 24. *Verificaremos se $F_4 = 65\,537$ é de fato primo. Temos que $3^{(F_4-1)/2} = 3^{32\,768} \equiv -1 \pmod{65\,537}$. Logo, pelo Teste de Pépin (Teorema 23), F_4 é primo.*

Mesmo não sabendo se um número de Fermat (generalizado) é primo ou composto, podemos ter informações sobre alguns de seus fatores. Por exemplo, se $n \geqslant 2$, então todo fator primo de $a^{2^n} + 1$ é da forma $p = h \cdot 2^{n+1} + 1$. De fato, se $p \mid a^{2^n} + 1$ é primo, então $a^{2^n} \equiv -1 \pmod{p} \implies a^{2^{n+1}} \equiv 1 \pmod{p}$. Assim, $\mathrm{ord}_p(a) = 2^{n+1}$. Por outro lado, $\mathrm{ord}_p(a) \mid p-1$ pela Proposição 7. Dessa forma, existe $h \in \mathbb{N}$ tal que $p - 1 = h \cdot 2^{n+1}$, isto é, $p = h \cdot 2^{n+1} + 1$.

Exemplo 25. $F_5 = 2^{2^5} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$. *Note que* $641 = 10 \cdot 2^6 + 1$.

O seguinte teste determinístico de primalidade aplica-se aos números de Proth:

Teorema 26 (Proth (1878))**.** *Seja $n = h \cdot 2^k + 1$, com $2^k > h$. Então n é primo se, e somente se, existe um $a \in \mathbb{N}$ tal que $a^{(n-1)/2} \equiv -1 \pmod{n}$.*

Demonstração. Se n é primo, basta escolher um a dentre os inteiros de 1 até $n-1$ tal que $\left(\frac{a}{n}\right) = -1$, então $a^{(n-1)/2} \equiv -1 \pmod{n}$ pelo critério de Euler (Teorema 10). Como $n = h \cdot 2^k + 1$, podemos escrever $n - 1 = h \cdot 2^k$. Se existe a tal que $a^{(n-1)/2} \equiv -1 \pmod{n}$, então $a^{n-1} \equiv 1 \pmod{n}$ e $\mathrm{mdc}(a^{(n-1)/2} - 1, n) = 1$. Logo, pelo Teorema 18, n é primo. $Q.E.D.$

Exemplo 27. *Como* $9\,857 = 77 \cdot 2^7 + 1$ *e* $2^7 > 77$. *Se conseguirmos encontrar um* $a \in \mathbb{N}$ *tal que* $a^{4\,928} \equiv -1 \pmod{9\,857}$, *então* $9\,857$ *é primo pelo Teorema de Proth (Teorema 26). Para* $a = 3$, $3^{4\,928} \equiv -1 \pmod{9\,857}$ *como queríamos. Portanto,* $9\,857$ *é primo.*

O próximo teste é uma generalização do anterior para um primo qualquer no lugar do 2.

Teorema 28. *Seja* $n = h \cdot p^k + 1$, *com* $p^k > h$ *potência de primo. Então* n *é primo se, e somente se, existe um* $a \in \mathbb{N}$ *tal que* $a^{n-1} \equiv 1 \pmod{n}$ *e* $\mathrm{mdc}(a^{(n-1)/p} - 1, n) = 1$.

Demonstração. Se n é primo, basta escolher um a dentre os inteiros de 1 até $n-1$ tal que $a \not\equiv x^p \pmod{n}$ para qualquer $x \in \mathbb{Z}$, então $a^{n-1} \equiv 1 \pmod{n}$ pelo Teorema 4 e também $a^{(n-1)/p} - 1 \not\equiv x^{n-1} - 1 \equiv 0 \pmod{n}$. Assim, n é primo e não é divisor de $a^{(n-1)/p} - 1$, portanto $\mathrm{mdc}(a^{(n-1)/p} - 1, n) = 1$. Se existe um $a \in \mathbb{N}$ tal que $a^{n-1} \equiv 1 \pmod{n}$ e $\mathrm{mdc}(a^{(n-1)/p} - 1, n) = 1$, então basta tomar $m = p^k$ e, pelo Teorema 18, n é primo. $Q.E.D.$

4. TESTE DOS PRIMOS DE MERSENNE

Nesta seção, vamos apresentar os primos de Mersenne, que estão entre os maiores primos conhecidos atualmente, e os testes determinísticos de primalidade aplicáveis a tais números.

Definição 29. *Um* número de Mersenne *é um número da forma* $M_p = 2^p - 1$. *Um* primo de Mersenne *é um número de Mersenne que é primo.*

Proposição 30. *Se* $2^n - 1$ *é primo, então* n *é primo.*

Demonstração. Supondo que n é composto, existem $a, b \geqslant 2$ inteiros tais que $n = a \cdot b$. Logo, $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1$. Dessa forma, temos $2^n - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \pmod{2^a - 1}$, isto é, $2^a - 1 \mid 2^n - 1$. Logo, por contraposição, n é primo se $2^n - 1$ é primo. $Q.E.D.$

A proposição anterior reduz a busca de primos de Mersenne para o caso em que o expoente n é primo. No entanto, observe que se n é primo, então $2^n - 1$ não é necessariamente primo. Isso ocorre, por exemplo, com $n = 11$, pois M_{11} é composto, como provaremos no Exemplo 32.

Não se sabe até hoje se existem infinitos primos de Mersenne ou não, mas dos 20 maiores primos conhecidos atualmente, 12 são de Mersenne, incluindo os 6 primeiros (sendo $2^{82\,589\,933} - 1$ o maior primo conhecido até o momento em que esse artigo está sendo escrito). Isso deve-se à eficiência do seguinte critério:

Teorema 31 (Critério de Lucas-Lehmer). *Sejam* $n > 2$ *e* S_n *tal que* $S_0 = 4$ *e* $S_{n+1} = S_n^2 - 2$. $M_n = 2^n - 1$ *é primo se, e somente se,* S_{n-2} *é múltiplo de* M_n.

Demonstração. Primeiro iremos verificar, por indução, que $S_n = (2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n}$: Para $n = 0$, $S_0 = (2 + \sqrt{3})^{2^0} + (2 - \sqrt{3})^{2^0} = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4$. Supondo $S_n = (2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}$, temos $S_{n+1} = ((2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n})^2 - 2 = (2+\sqrt{3})^{2^{n+1}} + 2 \cdot 1^{2^n} + (2 - \sqrt{3})^{2^{n+1}} - 2$. Então, $S_{n+1} = (2 + \sqrt{3})^{2^{n+1}} + (2 - \sqrt{3})^{2^{n+1}}$. Assim, pelo Princípio da Indução Finita, $S_n = (2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n}$ para todo n natural.

Supondo que S_{n-2} é múltiplo de M_n, isto é, $M_n \mid S_{n-2}$ e M_n composto, com um fator primo q tal que $q^2 \leqslant M_n$. Temos que $q \mid S_{n-2}$, então $S_{n-2} = (2 + \sqrt{3})^{2^{n-2}} + (2 - \sqrt{3})^{2^{n-2}} \equiv 0$

$(\mathrm{mod}\ q)$, o que implica que $(2+\sqrt{3})^{2^{n-2}} = -(2-\sqrt{3})^{2^{n-2}}$ em $G = (\mathbb{Z}[\sqrt{3}]/q)^\times$. E como $(2-\sqrt{3}) = (2+\sqrt{3})^{-1}$, temos $(2+\sqrt{3})^{2^{n-1}} = -1$ e $(2+\sqrt{3})^{2^n} = 1$ em G. Assim, a ordem de $(2+\sqrt{3})$ em G é 2^n, o que é absurdo, já que G possui no máximo $q^2-1 \leqslant M_n - 1 = 2^n - 2 < 2^n$ elementos. Assim, S_{n-2} é múltiplo de M_n implica que $M_n = 2^n - 1$ é primo.

Supondo agora M_n primo, com $n > 2$, temos que n é primo pela Proposição 30. Assim, $2^{n-1} \equiv 1 \pmod{n}$ pelo Teorema 4, o que significa que $n \mid 2^{n-1} - 1$. Como $2^n \equiv 1 \pmod{M_n}$, temos $2^{2^{n-1}-1} \equiv 1 \pmod{M_n}$, o que equivale a $(1+\sqrt{3})(1-\sqrt{3}) \equiv -2^{2^{n-1}} \pmod{M_n}$. Dado que M_n é primo, conclui-se pelo Pequeno Teorema de Fermat (5) que:

$$(1+\sqrt{3})^{M_n} \equiv 1 + (\sqrt{3})^{M_n} \equiv 1 + 3^{(M_n-1)/2}\sqrt{3} \equiv 1 + \left(\frac{3}{M_n}\right)\sqrt{3}$$

pelo Critério de Euler (Teorema 10) e, pelo Teorema 12, que $(1+\sqrt{3})^{M_n} \equiv 1 - \sqrt{3} \pmod{M_n}$.

Assim, $(1+\sqrt{3})^{M_n+1} \equiv (1+\sqrt{3})(1-\sqrt{3}) \equiv -2^{2^{n-1}} \pmod{M_n}$, o que implica que:

$$-1 \equiv \frac{(1+\sqrt{3})^{2^n}}{2^{2^{n-1}}} \equiv \left(\frac{(1+\sqrt{3})^2}{2}\right)^{2^{n-1}} \equiv (2+\sqrt{3})^{2^{n-1}} \pmod{M_n},$$

isto é, $(2+\sqrt{3})^{2^{n-2}} \equiv -(2-\sqrt{3})^{2^{n-2}} \pmod{M_n}$. Portanto, $(2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}} \equiv 0 \pmod{M_n}$, isto é, $M_n = 2^n - 1$ ser primo implica que $M_n \mid S_{n-2}$. $Q.E.D.$

Exemplo 32. *Verificaremos a primalidade do número de Mersenne $M_{11} = 2\,047$. Primeiro precisamos encontrar o termo S_9 da sequência. Como $S_n = (2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}$, então $S_9 = (2+\sqrt{3})^{2^9} + (2-\sqrt{3})^{2^9} \equiv 493 \pmod{2\,047}$. Portanto, pelo Critério de Lucas-Lehmer (Teorema 31), $M_{11} = 2\,047$ não é primo.*

Mesmo não sabendo se um certo número de Mersenne é primo ou não, podemos determinar a forma dos seus divisores primos através da próxima proposição, que usaremos para encontrar os fatores de $2\,047$.

Proposição 33. *Sejam $p, q > 2$ primos, com $q \mid M_p$. Então, $q \equiv 1 \pmod{p}$ e $q \equiv \pm 1 \pmod{8}$.*

Demonstração. Como $q \mid M_p = 2^p - 1$, então $2^p \equiv 1 \pmod{q}$, o que significa que $\mathrm{ord}_q(2) = p$, pois p é primo. Assim, $p \mid q - 1 = \varphi(q)$ e, portanto, $q \equiv 1 \pmod{p}$. De $2^p \equiv 1 \pmod{q}$ também podemos concluir que $2 \equiv 2^{p+1} = (2^{\frac{p+1}{2}})^2 \pmod{q}$, o que garante pela Proposição 11 que $\left(\frac{2}{q}\right) = 1$ e, portanto, $q \equiv \pm 1 \pmod{8}$ pelo Teorema 12. $Q.E.D.$

Exemplo 34. *Como $M_{11} = 2\,047$, então qualquer fator primo q de $2\,047$ deve ser tal que $q \equiv 1 \pmod{11}$ e $q \equiv \pm 1 \pmod{8}$. A primeira congruência nos garante que $q \in \{12, 23, 34, 45, \ldots\}$. O primeiro primo dessa lista é 23, que é $23 \equiv -1 \pmod{8}$. De fato, 23 é um fator primo de $2\,047$. O outro fator, $89 = 2\,047 \div 23$, também é tal que $89 \equiv 1 \pmod{11}$ e $89 \equiv 1 \pmod{8}$.*

5. TESTE AKS

Nesta seção, vamos apresentar a versão de Lenstra para o Teste AKS (devido a Agrawal, Kayal e Saxena). Assim como todos os testes determinísticos apresentados aqui e os probabilísticos

mais eficientes até hoje, o Teste AKS baseia-se no Pequeno Teorema de Fermat (Teorema 5). De fato, se x é uma variável e $a \in \mathbb{Z}$, então vale $(x+a)^p = x^p + a$ em $\mathbb{Z}_p[x]$, com p primo. Logo,

$$\begin{aligned} n \text{ é primo} &\iff (x+a)^n \equiv x^n + a \pmod{n} \text{ para todo } a \text{ tal que } 1 \leqslant a < n \\ &\iff (x+a)^n \equiv x^n + a \pmod{n} \text{ para algum } a \text{ com } 1 \leqslant a < n \text{ e } \operatorname{mdc}(a,n) = 1. \end{aligned}$$

Por outro lado, se $(x+a)^n = x^n + a$ em $\mathbb{Z}_p[x]$, então $(x+a)^n \equiv x^n + a \pmod{n}$ e $(x+a)^n \equiv x^n + a \pmod{x^r - 1}$ para todo $r \in \mathbb{N}$. Segue do resultado de AKS que para garantir a primalidade de n, basta testar a congruência anterior para um valor especial de r.

Teorema 35 (Agrawal, Kayal, Saxena, Lenstra)**.** *Sejam $n, r > 1$ inteiros, com r potência de primo, e S um subconjunto finito dos naturais com s elementos menores do que n. Se supormos que:*

i) n *e* r *são coprimos e* $\operatorname{ord}_r(n) = v > 1$;

ii) $\operatorname{mdc}(n, a-b) = 1$, *para* $a, b \in S$, *com* $a \neq b$;

iii) $\binom{s+t-1}{s} \geqslant n^{\sqrt{t/2}}$, *para todo* t *divisor de* $\varphi(r)$ *e múltiplo de* v;

iv) $(x+a)^n \equiv x^n + a \pmod{n}$ *e* $(x+a)^n \equiv x^n + a \pmod{x^r - 1}$, *para* $a \in S$;

Então n é potência de um primo.

Demonstração. Por (i), existe um divisor primo de p tal que $\operatorname{ord}_r(p) > 1$; pois, caso contrário, $p \equiv 1 \pmod{r}$ para todo primo p divisor de n e, assim, $n \equiv 1 \pmod{r}$, isto é, $\operatorname{ord}_r(n) = 1$, o que é um absurdo, já que $\operatorname{ord}_r(n) = v > 1$ por hipótese. Por (iv), $(x+a)^n = x^n + a$ no anel $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$ para todo $a \in S$. Substituindo na expressão anterior x por x^{n^i}, obtemos $(x^{n^i} + a)^n = x^{n^{i+1}} + a$ no anel $\mathbb{Z}_p[x]/\langle x^{rn^i} - 1\rangle$. Como $(x^r - 1) \mid (x^{rn^i} - 1)$, podemos escrever que $(x^{n^i} + a)^n = x^{n^{i+1}} + a$ no anel $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$. Por indução, concluímos que $(x+a)^{n^i} = x^{n^i} + a$ no anel $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$ para todo $a \in S$. Pelo Pequeno Teorema de Fermat (5), $(x+a)^{n^i p^j} = (x^{n^i} + a)^{p^j} = x^{n^i p^j} + a$ e, portanto, $(x+a)^{(n/p)^i p^j} = x^{(n/p)^i p^j} + a$ no anel $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$ para todo $a \in S$.

Seja $G = \langle n, p\rangle$ o subgrupo multiplicativo de $\mathbb{Z}_r^\times$ gerado pelas classes de congruência de n e de p módulo r, e seja $t = |G|$. Temos que $t \mid \varphi(r) = \left|\mathbb{Z}_r^\times\right|$ e $\left|\langle n\rangle \pmod{r}\right| = \operatorname{ord}_r(n) = v \mid t$, pois a ordem de um subgrupo divide a ordem do seu grupo. Mostraremos que existem mais do que t pares $i, j \geqslant 0$ tais que $(n/p)^i p^j \leqslant n^{\sqrt{t/2}}$:

Considere o triângulo T formado pelos pontos $(x, y) \in \mathbb{R}^2$ com $x, y \geqslant 0$ tais que $(n/p)^x p^y \leqslant n^{\sqrt{t/2}}$. A área do triângulo T é

$$\frac{t \log^2(n)}{4 \log(n/p) \log(p)} \geqslant t,$$

que é menor do que a quantidade de quadrados da forma $[i, i+1] \times [j, j+1]$ com $i, j \geqslant 0$ inteiros tais que $(n/p)^i p^j \leqslant n^{\sqrt{t/2}}$, provando assim a nossa afirmação.

Como há mais do que $t = |G|$ pares (i, j) e $G = \langle n, p\rangle \pmod{r} = \langle n/p, p\rangle \pmod{r}$, então existem dois pares (i, j) e (k, ℓ) tais que $(n/p)^i p^j \equiv (n/p)^k p^\ell \pmod{r}$. Denotando por $w = (n/p)^i p^j$ e $u = (n/p)^k p^\ell$, temos $x^w = x^u$ em $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$ e $|w - u| < n^{\sqrt{t/2}}$. Logo, para todo $a \in S$, $(x+a)^w = x^w + a = x^u + a = (x+a)^u$ em $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$.

Como r é potência de primo, por hipótese, podemos escrever $r = q^d$, com q primo e $d \in \mathbb{N}$. Seja $h(x)$ um polinômio irredutível em $\mathbb{Z}_p[x]$ que divide o seguinte polinômio:

$$x^{q^d - q^{d-1}} + x^{q^d - 2q^{d-1}} + \cdots + x^{2q^{d-1}} + x^{q^{d-1}} + 1 = \frac{x^{q^d} - 1}{x^{q^{d-1}} - 1}.$$

O corpo $K = \mathbb{Z}_p[x]/\langle h(x)\rangle$ possui $p^{\partial h(x)}$ elementos, em que $\partial h(x)$ é o grau do polinômio $h(x)$. Em K, $\dfrac{x^{q^d} - 1}{x^{q^{d-1}} - 1} = 0$, isto é, $x^{q^d} = 1$ e $x^{q^{d-1}} \neq 1$, o que significa que $\operatorname{ord}(x) = q^d = r$. Assim, $r \mid p^{\partial h(x)} - 1$, o que implica que $p \equiv 1 \pmod{r}$ e, portanto, $\operatorname{ord}_r(p) \mid \partial h(x)$, o que significa que $\partial h(x) > 1$. Seja H o subgrupo de $K^\times$ gerado pelos elementos $x + a$, com $a \in S$. Garantimos que os elementos $x + a$ são todos distintos em K.

Um polinômio $f \in \mathbb{Z}_p[y]$ é chamado *introspectivo* se $f(y^p) \equiv (f(y))^p$ e $f(y^{n/p}) \equiv (f(y))^{n/p} \pmod{y^r - 1}$. O produto de polinômios introspectivos também é introspectivo e, pelo que já vimos, $y + a$ é introspectivo para $a \in S$. Considerando os multi-índices $E = (e_a)_{a \in S}$, com $e_a \in \mathbb{N}$ para todo $a \in S$ que satisfazem $\displaystyle\sum_{a \in S} e_a \leqslant t - 1$, e seja $P_E(y) = \displaystyle\prod_{a \in S} (y + a)^{e_a} \in \mathbb{Z}_p[y]$ para cada E, teremos que estes polinômios também são introspectivos. É fácil notar que os elementos $P_E(x) \in K$ são todos distintos.

Assim, H tem no mínimo $\dbinom{s + t - 1}{s} \geqslant n^{\sqrt{t/2}} > |w - u|$ elementos. Como temos que $m^w = m^u$ para todo $m \in H$, mas se $w \neq u$, então a equação pode ter no máximo $|w - u|$ soluções não nulas num corpo, o que é um absurdo. Logo, $w = u$, isto é, $(n/p)^i p^j = (n/p)^k p^\ell$. Como $i \neq k$ (pois caso contrário, $i = k \implies j = \ell$ e, portanto, $(i, j) = (k, \ell)$, o que não ocorre), então concluímos de $(n/p)^i p^j = (n/p)^k p^\ell$ que n é potência de p. $Q.E.D.$

6. CONCLUSÃO

Neste artigo, vimos o que são os testes determinísticos de primalidade e alguns exemplos. Esses testes dão a certeza se que um número n grande é primo ou não. Na prática, são computacionalmente mais lentos do que os probabilísticos, fazendo-se necessário uma combinação dos dois tipos de testes: inicialmente, usamos um probabilístico para reduzir a lista de possibilidades dos números a serem testados, em seguida, usamos um determinístico para termos a certeza de quem é ou não primo.

Apesar de serem, em geral, mais lentos que os testes probabilísticos, os testes determinísticos podem ser mais eficientemente aplicados a determinadas classes de números. Dos 20 maiores primos conhecidos atualmente, 12 são de Mersenne, 2 são de Proth, 2 são de Fermat generalizados e 4 são de outros tipos, tendo sido apresentados neste artigo justamente os testes usados para essas classes de números.

7. AGRADECIMENTOS

Agradeço primeiramente a Deus e aos meus pais, Rodlon e Luciane, pelas oportunidades que me permitiram dedicar-me ao estudo da Matemática. Agradeço também ao meu orientador, Sávio Ribas, pelos ensinamentos e pela ajuda na escrita deste artigo. Por fim, agradeço também ao grupo PETMAT, do qual já fui membro, por estar promovendo a II Mostra de Iniciação Científica em Matemática da UFOP.

8. REFERÊNCIAS

COUTINHO, S. C. **Números inteiros e criptografia RSA**. [S.l.]: IMPA, 2014. (Coleção Matemática e Aplicações). ISBN 9788524401244.

GONçALVEZ, A. **Introdução à Álgebra**. [S.l.]: IMPA, 2009. (Projeto Euclides). ISBN 9788524401084.

LIDL, R.; NIEDERREITER, H. **Finite Fields**. [S.l.]: Cambridge, 1997. (Cambridge University Press). ISBN 0521392314.

MARTINEZ, F. B.; MOREIRA, C. G.; SALDANHA, N.; TENGAN, E. **Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro**. [S.l.]: SBM, 2024. (Coleção Textos Universitários). ISBN 9788583372295.

RIBENBOIM, P. **Números primos. Velhos mistérios e novos recordes**. [S.l.]: IMPA, 2014. (Coleção matemática universitária). ISBN 9788524403347.