2015: Trabalho de Conclusão de Curso do Mestrado Profissional em Matemática - PROFMAT
Universidade Federal de São João del-Rei - UFSJ
Sociedade Brasileira de Matemática - SBM

UM CRITÉRIO DE PRIMALIDADE BASEADO NO TEOREMA DE WILSON

Waldilainy de Campos [1]
Jorge Andrés Julca Avila[2]

Resumo: Neste trabalho, estudamos um dos assuntos mais instigantes da matemática, *os números primos*. Apresentaremos um novo resultado de teste de primalidade de um número, baseado no Teorema de Wilson, [8]. Iniciamos com alguns resultados importantes da teoria de números com a finalidade de demonstrar o Teorema de Wilson e, fundamentalmente, o *Teorema Principal*, o qual, reduz o número de operações realizadas pelo Teorema de Wilson.

Palavras-chave: Números Primos, Teste de Primalidade, Teorema de Wilson.

1 Introdução

Há mais de dois mil anos as civilizações já utilizavam cálculos em sua rotina para desenvolver algumas atividades, dentre elas, comércio e construção. Não existe registro de como esses cálculos eram feitos porém podemos imaginar que um dos meios utilizados possa ter sido a fatoração dos números [6], [7]. Mesmo com a utilidade deste método, surge o problema de que alguns números não são fatoráveis, começando então, a ideia de número primo. Em latim, primo significa primeiro, por isso, os números primos foram batizados com esse nome. Apesar de que o mais justo seria que fossem chamados de números atômicos, em grego, indivisível.

Desde seu conhecimento, os números primos permanecem como um dos assuntos mais enigmáticos já estudados pelos matemáticos em todo o mundo. Em uma ciência dedicada a encontrar normas e regras, os números primos permanecem como um desafio absoluto. Basta observarmos que sua sequência 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,... é irregular, sem lógica, com números aleatórios e não há nenhuma indicação que nos permita prever qual será o próximo número primo.

Várias questões relacionadas aos números primos vêm provocando as mentes de matemáticos em todo o mundo. Algumas questões já foram resolvidas na Antiguidade, como a prova de sua infinitude [5] e o crivo de Eratóstenes que gera primos inferiores a um número natural dado [4]; outras questões continuam em aberto como é o caso da Hipótese de Riemann [1], que é apontado como um dos maiores problemas do milênio e é uma dessas questões que perdura por mais de um século e meio sem resultado. A hipótese está ligada com a distribuição dos números primos e sua solução tornará possível entender o comportamento de sua sequência

[1]Aluna de Mestrado Profissional em Matemática, Turma 2013
Instituição: Universidade Federal de São João del-Rei - UFSJ
E-mail: wwfeliz@hotmail.com
[2]Orientador do Trabalho de Conclusão de Curso
Departamento de Matemática e Estatística - DEMAT, UFSJ
E-mail: avila_jaj@ufsj.edu.br

permitindo provar muitos resultados que dependem de sua confirmação.

No mundo dos números primos existem pelo menos dois grandes problemas: a *distribuição dos números primos* e os *testes de primalidade*, os quais estão intimamente interligados.

Por outro lado, devido a seu grau de complexidade, os números primos vêm ganhando importância em uma aplicação prática, desconhecida pela maioria e utilizada por todos nós: *os sistemas de segurança online*. Esses sistemas geram códigos utilizando números primos com um número alto de algarismos que servem para proteger senhas, informações pessoais, operações bancárias e qualquer transmissão online de dados. Os números primos são os tesouros que escondem os sigilos eletrônicos do mundo globalizado.

Neste trabalho, apresentaremos um novo teorema que contribui com um dos grandes problemas dos números primos, chamados testes de primalidade. Antes de sua apresentação fizemos uma pequena viagem pela história desses misteriosos números e sua utilização prática. Baseado no Teorema de Wilson, o Teorema Principal deste trabalho testa a primalidade de um número e para sua demonstração fez-se necessária a apresentação de alguns resultados importantes da teoria de números, como definições, proposições e a demonstração do próprio Teorema de Wilson. Enfim, com o intuito de reforçar a ideia esperada pelo novo teorema, fizemos uma análise comparativa entre o Teorema de Wilson e o Teorema Principal, quanto à quantidade de cálculo utilizado.

2 Preliminares

Enunciaremos algumas definições e proposições que serão necessários para a demonstração do Teorema de Wilson e do Teorema Principal deste trabalho.

Definição 2.1 (Números Naturais e Números Inteiros) Os números naturais são definidos pelo seguinte conjunto:

$$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}.$$

Denotaremos $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Os números inteiros são definidos pelo seguinte conjunto:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

Proposição 2.1 $\forall n \in \mathbb{N}^*, (2n)! > (n!)^2$.

Demonstração: A demonstração será feita por Indução Finita.

- Para $n = 1$, é válido que

$$(2 \cdot 1)! = 2! = 2 > 1 = 1! = (1!)^2.$$

- Para $n = k$, consideremos a *hipótese indutiva*,

$$(2k)! > (k!)^2.$$

- Utilizando tal hipótese, demonstraremos que

$$[2(k+1)]! > [(k+1)!]^2.$$

Com efeito,

$$\begin{aligned}
[2(k+1)]! &= (2k+2)! = (2k+2)(2k+1)(2k)! \\
&> (2k+2)(2k+1)(k!)^2 \\
&= 2(k+1)(2k+1)(k!)^2 \\
&> 2(k+1)(k+1)(k!)^2 \\
&> (k+1)(k+1)(k!)^2 \\
&= (k+1)^2(k!)^2 = [(k+1)(k!)]^2 = [(k+1)!]^2
\end{aligned}$$

□

Definição 2.2 (Números Primos) Um número natural p é chamado de número primo quando possui apenas dois divisores: o número 1 e o próprio número p.
Denotaremos o conjunto dos números primos por

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, ...\}$$

e o conjuntos dos números primos ímpares por $\mathcal{P}^* = \mathcal{P} \setminus \{2\}$.

***Observação* 2.1** (x, m) denota o máximo divisor comum de x e m.

Definição 2.3 (Congruência módulo m) Sejam a e b números inteiros quaisquer e m um número natural positivo. Podemos dizer que a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Escreve-se:

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

***Observação* 2.2** Consideraremos sempre $m > 1$ pois o resto da divisão de qualquer número inteiro por 1 será sempre nulo.

Exemplo 2.1 Os números 18 e 33 são congruentes módulo 5 (isto é, $18 \equiv 33 \mod 5$) pois o resto da divisão de 18 por 5 é 3 e de 33 por 5 também é 3.

Definição 2.4 (Classe residual módulo m do elemento $a \in \mathbb{Z}$) O subconjunto dos números inteiros no qual todos os elementos possuem o mesmo resto quando divididos por m é chamado classe residual módulo m do elemento $a \in \mathbb{Z}$. Escreve-se:

$$[a] = \{x \in \mathbb{Z} : x \equiv a \mod m\}.$$

***Observação* 2.3** O conjunto de todas as classes residuais módulo m será representado por $\mathbb{Z}_m$. Escreve-se:

$$\mathbb{Z}_m = \{[0], [1], [2], ..., [m-1]\}.$$

***Observação* 2.4** Em Z_m definimos as seguintes operações:

Adição: $[a] + [b] = [a + b]$.
Multiplicação: $[a] \cdot [b] = [a \cdot b]$.

***Observação* 2.5** O elemento $[a] \in \mathbb{Z}_m$ será dito invertível quando existir $[x] \in \mathbb{Z}_m$, tal que $[a] \cdot [x] = [1]$. Neste caso, $[x]$ é o inverso multiplicativo de $[a]$.

***Observação* 2.6** Resolver a congruência $ax \equiv 1 \mod m$ equivale a resolver em $\mathbb{Z}_m$ a equação $[a] \cdot [x] = [1]$.

Proposição 2.2 *Sejam a, b, $m \in \mathbb{Z}$, com $m > 1$. Então,*

$$a \equiv b \mod m \iff m \mid b - a.$$

Uma demonstração da Proposição 2.2 é encontrada em [5] pág. 193.

Exemplo 2.2 $21 \equiv 11 \mod 2$ já que os restos da divisão de 21 e 11 por 2 são iguais a 1, também temos que $2|(11 - 21)$ que equivale a $2|(-10)$ ou ainda a $2|(10)$, ilustrando a proposição 2.2.

Proposição 2.3 *Sejam a, b, c, $m \in \mathbb{Z}$, com $m > 1$. Temos,*

$$a \equiv b \mod m \iff a + c \equiv b + c \mod m.$$

Demonstração: Seja $a \equiv b \mod m$. Nesse caso, temos que $m \mid b-a$. Somando e subtraindo c temos $m \mid b + c - a - c$ e portanto $m \mid (b + c) - (a + c)$. Logo, por definição $a + c \equiv b + c \mod m$. Reciprocamente, supondo $a + c \equiv b + c \mod m$, temos $m \mid a + c - (b + c)$. Logo $m \mid a - b$, o que equivale a $a \equiv b \mod m$. □

Proposição 2.4 *Se a, b, $c \in \mathbb{Z}$ são tais que $a \mid b$ e $a \mid c$, então $a \mid (xb + yc)$, $\forall\ x$, $y \in \mathbb{Z}$.*

Uma demonstração da Proposição 2.4 é encontrada em [5] pág. 48.

Proposição 2.5 *Sejam a, b, c, $m \in \mathbb{Z}$, com $m > 1$. Temos,*

$$a \equiv b \mod m \quad \text{e} \quad b \equiv c \mod m \implies a \equiv c \mod m.$$

Demonstração: Seja $a \equiv b \mod m$, temos que $m \mid b - a$. Seja $b \equiv c \mod m$, temos que $m \mid c - b$. Pela proposição 2.4, podemos afirmar que $m \mid b - a + c - b$. Logo, $m \mid -a + c$, o que equivale a $a \equiv c \mod m$. □

Exemplo 2.3 Temos $21 \equiv 15 \mod 2$ e $15 \equiv 19 \mod 2$. Daí 21, 15 e 19 possuem o mesmo resto quando divididos por 2. Logo $21 \equiv 19 \mod 2$.

Proposição 2.6 *Sejam a, b, c, d, $m \in \mathbb{Z}$, com $m > 1$. Então,*

$$a \equiv b \mod m \quad \text{e} \quad c \equiv d \mod m \implies ac \equiv bd \mod m.$$

Demonstração: Temos que $m \mid b - a$. Multiplicando $b - a$ por c, temos $m \mid bc - ac$. Logo $ac \equiv bc \mod m$. Por outro lado, temos que $m \mid d - c$ e multiplicando $d - c$ por b, obtemos $m \mid bd - bc$, isto é $bc \equiv bd \mod m$. Aplicando a Proposição 2.5, temos que $ac \equiv bd \mod m$. □

Proposição 2.7 *Sejam a, b, m, $x \in \mathbb{Z}$, com $m > 1$ e $x \neq 0$. Temos,*

$$ax \equiv bx \mod m \iff a \equiv b \mod \frac{m}{(x,m)}.$$

Uma demonstração da Proposição 2.7 é encontrada em [3] pág. 56.

Exemplo 2.4 Temos $20 \equiv 12 \mod 8$, o que é $5 \cdot 4 \equiv 3 \cdot 4 \mod 8$. Sabemos que $(4, 8) = 4$ e que $5 \equiv 3 \mod 2$, ilustrando o resultado da Proposição 2.7.

Proposição 2.8 *Sejam a, b, n, $m \in \mathbb{Z}$, com $m > 1$ e $n > 1$. Temos,*

$$a \equiv b \mod m \quad \text{e} \quad n \mid m \implies a \equiv b \mod n.$$

Demonstração: Se $a \equiv b \mod m$, então $m \mid b - a$. Como $n \mid m$, segue-se que $n \mid b - a$. Logo, $a \equiv b \mod n$. □

Proposição 2.9 *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros x e y tais que $ax - by = 1$.*

Uma demonstração da Proposição 2.9 é encontrada em [5] pág. 96.

Proposição 2.10 *$[a] \in \mathbb{Z}_m$ é invertível se, e somente se, $(a, m) = 1$.*

Demonstração: Se $[a]$ é invertível, então existe $[x] \in \mathbb{Z}_m$ tal que $ax \equiv 1 \mod m$. Logo, $m \mid ax - 1$, isto é, existe $y \in \mathbb{Z}$ tal que $ax - my = 1$, logo $(a, m) = 1$. Reciprocamente, se $(a, m) = 1$, temos x, $y \in \mathbb{Z}$ tais que $ax - my = 1$ e, consequentemente, $[1] = [ax - my] = [ax] - [my] = [a] \cdot [x] - [0] = [a] \cdot [x]$. Portanto, $[a]$ é invertível. □

***Observação* 2.7** Da Proposição 2.10 temos que, se $(a, m) = 1$ então a congruência $ax \equiv 1 \mod m$ possui solução única, isto é, o inverso multiplicativo x é único. De fato, se $ax_0 \equiv 1 \mod m$ e $ax_1 \equiv 1 \mod m$, então $ax_0 \equiv ax_1 \mod m$. Como $(a, m) = 1$, pela Proposição 2.7 temos que $x_0 \equiv x_1 \mod m$, o que equivale a $[x_1] = [x_0]$ em $\mathbb{Z}_m$.

***Observação* 2.8** $x^2 \equiv 1 \mod p \iff x \equiv \pm 1 \mod p$, com p primo. Provaremos ($\Rightarrow$): $x^2 \equiv 1 \mod p$ é equivalente a $p|(x^2 - 1)$, o qual implica, $p|(x + 1)$ ou $p|(x - 1)$. Assim, $x \equiv 1 \mod p$ ou $x \equiv -1 \mod p$. Agora, ($\Leftarrow$): $x \equiv \pm 1 \mod p$, pela proposição 2.6, $x^2 \equiv (\pm 1)^2 = 1 \mod p$.

Proposição 2.11 *Sejam a, $b \in \mathbb{Z}$ e $p \in \mathcal{P}$. Então,*

$$p \mid ab \implies p|a \quad \text{ou} \quad p \mid b.$$

Demonstração: Se $p|ab$, então existe $m \in \mathbb{Z}$, tal que $ab = pm$. Por outro lado, suponha primeiro que a e p sejam primos entre si, isto é, $(a, p) = 1$. Pela Proposição 2.9 temos que $ax - py = 1$. Multiplicando, esta última expressão, por b temos que $abx - bpy = b$. Substituindo ab por pm temos que $pmx - byp = b$. Logo $b = p(mx - yp)$, assim, $p|b$. O caso $p|a$ é análogo. □

Proposição 2.12 *Todo número primo ímpar é da forma $4k + 1$ ou $4k + 3$, $k \in \mathbb{N}$.*

Demonstração: Seja $n \in \mathbb{N}$, dividindo n por 4, teremos os possíveis restos: 0, 1, 2 ou 3. Então, as possibilidades para n serão: $4k$, $4k+1$, $4k+2$ ou $4k+3$. Como todo primo maior que 2 é ímpar, os números primos ímpares serão da forma $4k+1$ ou $4k+3$, pois $4k$ e $4k+2$ são números pares. □

***Observação* 2.9** A recíproca da Proposição 2.12 não é verdadeira, pois nem todo número da forma $4k+1$ e $4k+3$ é primo. Por exemplo, 15 é da forma $4k+3$ com $k=3$ e não é um número primo. O número 21 é da forma $4k+1$ com $k=5$ e também não é um número primo.

3 Teorema de Wilson

John Wilson (1741 - 1793), nascido na Inglaterra, foi professor de matemática, porém abandonou a carreira para estudar direito, se tornando juiz. Ficou conhecido pela elaboração do Teorema de Wilson, demonstrado pioneiramente por Joseph Louis Lagrange (1736 - 1813). Em Figura 1, temos um retrato de John Wilson.

Figura 1: Retrato de John Wilson, [9].

A seguir enunciaremos uma dos grandes teoremas de teste de primalidade, devido a John Wilson.

Teorema 3.1 (Teorema de Wilson)

$$p \in \mathcal{P} \iff (p-1)! \equiv -1 \mod p. \tag{1}$$

Demonstração: ($\Rightarrow$)Para $p=2$ ou $p=3$ o resultado é facilmente verificável. Para $p>3$, considere $a \in \{1,2,3,...,p-1\}$, logo $(a,p)=1$. Pela Proposição 2.10 e Observação 2.7, temos que a congruência $ax \equiv 1 \mod p$ possui solução única módulo p, ou seja, para cada $a \in \{1,2,3,...,p-2,p-1\}$ existe um único $x \in \{1,2,3,...,p-2,p-1\}$ que satisfaz a congruência. Afirmamos que a equação $ax \equiv 1 \mod p$ não é satisfeita por $x=a$, exceto se $a=1$ ou $a=p-1$. De fato, se tivéssemos $x=a$, teríamos $a^2 \equiv 1 \mod p$ e consequentemente, pela observação 2.8, $a \equiv 1 \mod p$ ou $a \equiv p-1 = -1 \mod p$. Consequentemente, $x = \pm 1$ não é solução de $ax \equiv 1 \mod p$ se $a \neq 1$ e $a \neq p-1$.

Dessa forma para cada $a \in \{2,3,4,...,p-2\}$ existe um único $x \in \{2,3,4,...,p-2\}$ que é solução de $ax \equiv 1 \mod p$. Então, podemos reordenar o conjunto $\{2,3,4,...,p-2\}$, isto é,

$$\{2,3,4,...,p-2\} = \{i_1, j_1, i_2, j_2, ..., i_{\frac{p-3}{2}}, j_{\frac{p-3}{2}}\}$$

em que, $i_1 j_1 \equiv i_2 j_2 \equiv ... \equiv i_{\frac{p-3}{2}} j_{\frac{p-3}{2}} \equiv 1 \mod p$. Ou seja, j_t é o inverso de i_t, $t = 1, 2, ...\frac{p-3}{2}$. Daqui, $i_1 j_1 i_2 j_2 ... i_{\frac{p-3}{2}} j_{\frac{p-3}{2}} \equiv 1 \mod p$. Assim,

$$2 \cdot 3 \cdot 4 \cdot ... \cdot (p-2) \equiv 1 \mod p$$

de modo que,

$$1 \cdot 2 \cdot 3 \cdot ... \cdot (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \mod p$$

e finalmente,

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

logo,

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

($\Leftarrow$) Suponhamos que $(p-1)! \equiv -1 \mod p$, com $p = mn$ composto. Então, pela Proposição 2.8, podemos escrever $(p-1)! \equiv -1 \mod m$. Por outro lado, como $m < p$ e $m \neq 1$ então $m \in \{p-1, p-2, ..., 2\}$. Assim, $m \mid (p-1)!$ e portanto $(p-1)! \equiv 0 \mod m$. Consequentemente, $0 \equiv -1 \mod m$, o que é um absurdo, então não existe tal fator m. Concluindo-se que p é primo. □

Exemplo 3.1 O número 11 é primo. De fato, primeiro verificaremos que o número 11 satisfaz a congruência $(p-1)! \equiv -1 \mod p$, ou seja, $(11-1)! \equiv -1 \mod 11 \iff 10! \equiv -1 \mod 11 \iff 3.628.800 \equiv -1 \mod 11 \iff 11|(3.628.800+1) \iff 11|(329.801 \times 11)$. Assim, 11 satisfaz a congruência (1). Logo, pelo Teorema de Wilson, 11 é um número primo.

4 Teorema Principal

Enunciaremos o Teorema Principal deste trabalho, estabelecido em [8]. Este teorema nos fornece um novo teste de primalidade.

Teorema 4.1 (Teorema Principal)

$$p \in \mathcal{P}^* \iff \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \mod p. \tag{2}$$

Demonstração:
Desenvolvendo o termo $(p-1)!$, temos:

$$\begin{aligned}
(p-1)! &= 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-2) \cdot (p-1) \\
&= 1 \cdot 2 \cdot 3 \cdot ... \cdot \left(\frac{p-1}{2}\right) \cdot \left(p - \frac{p-1}{2}\right) \cdot ... \cdot p - 1 \\
&= 1(p-1) \cdot 2(p-2) \cdot 3(p-3) \cdot ... \cdot \left(\frac{p-1}{2}\right) \cdot \left(p - \frac{p-1}{2}\right) \\
&= (1p - 1^2) \cdot (2p - 2^2) \cdot (3p - 3^2) \cdot ... \cdot \left[\left(\frac{p-1}{2}\right)p - \left(\frac{p-1}{2}\right)^2\right]. \qquad (3)
\end{aligned}$$

Por outro lado,

$$\begin{aligned} 1p - 1^2 &\equiv -1^2 \mod p, \\ 2p - 2^2 &\equiv -2^2 \mod p, \\ 3p - 3^2 &\equiv -3^2 \mod p, \\ &\vdots \\ \left(\frac{p-1}{2}\right)p - \left(\frac{p-1}{2}\right)^2 &\equiv -\left(\frac{p-1}{2}\right)^2 \mod p. \end{aligned}$$

Pela Proposição 2.6,

$$(1p - 1^2) \cdot (2p - 2^2) \cdot (3p - 3^2) \cdot \ ... \ \cdot \left[\left(\frac{p-1}{2}\right)p - \left(\frac{p-1}{2}\right)^2\right] \equiv$$
$$(-1^2) \cdot (-2^2) \cdot (-3^2) \cdot ... \cdot \left[-\left(\frac{p-1}{2}\right)^2\right] \mod p. \quad (4)$$

Substituindo (3) em (4), temos

$$\begin{aligned} (p-1)! &\equiv (-1^2) \cdot (-2^2) \cdot (-3^2) \cdot ... \cdot \left[-\left(\frac{p-1}{2}\right)^2\right] \mod p \\ &= \underbrace{(-1) \cdot (-1) \cdot (-1) \cdot ... \cdot (-1)}_{\frac{p-1}{2} \text{ vezes}} \cdot (1^2) \cdot (2^2) \cdot (3^2) \cdot ... \cdot \left(\frac{p-1}{2}\right)^2 \mod p \\ &= (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \mod p. \end{aligned} \quad (5)$$

Agora, pelo Teorema de Wilson e por (5),

$$\begin{aligned} p \in \mathcal{P} &\iff (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \mod p \\ &\iff (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)(-1)^{\frac{p-1}{2}} \mod p \\ &\iff (-1)^{p-1} \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \mod p. \end{aligned} \quad (6)$$

Como p é ímpar, $(-1)^{p-1}$ será sempre igual a 1. Logo,

$$p \in \mathcal{P}^* \iff \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \mod p.$$

□

Pela Proposição 2.12 sabemos que os números primos ímpares são da forma $4k+1$ ou $4k+3$. Logo, podemos obter dois resultados do nosso Teorema Principal.

Corolário 1(Teorema de Sierpinsky). *Seja $p \in \mathcal{P}$. Então,*

$$p = 4k+1 \Longrightarrow \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \mod p. \tag{7}$$

Demonstração: Do Teorema Principal, temos $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$. Se $p = 4k+1$, então $(-1)^{\frac{p+1}{2}} = (-1)^{\frac{4k+1+1}{2}} = (-1)^{\frac{4k+2}{2}} = (-1)^{2k+1} = -1$. □

Corolário 2 *Seja $p \in \mathcal{P}$. Então,*

$$p = 4k+3 \Longrightarrow \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1 \mod p. \tag{8}$$

Demonstração: Do Teorema Principal, temos $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$. Se $p = 4k+3$, então $(-1)^{\frac{p+1}{2}} = (-1)^{\frac{4k+3+1}{2}} = (-1)^{\frac{4k+4}{2}} = (-1)^{2(k+1)} = 1$. □

***Observação* 4.1** Seja $p \in \mathcal{P}$. Então, $p = 4k+3 \Longrightarrow \left(\frac{p-1}{2}\right)! \equiv \pm 1 \mod p$. De fato, utilizando o Corolário 2 e Proposição 2.2, temos que

$$p \mid \left\{\left[\left(\frac{p-1}{2}\right)!\right]^2 - 1\right\} \Longleftrightarrow p \mid \left\{\left[\left(\frac{p-1}{2}\right)! - 1\right]\left[\left(\frac{p-1}{2}\right)! + 1\right]\right\}.$$

Então, usando a Proposição 2.11,

$$\left(\frac{p-1}{2}\right)! \equiv 1 \mod p \quad \text{ou} \quad \left(\frac{p-1}{2}\right)! \equiv -1 \mod p,$$

ou, equivalentemente,

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \mod p. \tag{9}$$

Exemplo 4.1 O número 11 é primo. De fato, primeiro verificaremos que o número 11 satisfaz a congruência $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$, ou seja, $\left[\left(\frac{11-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{11+1}{2}} \mod 11 \Longleftrightarrow (5!)^2 \equiv (-1)^6 \mod 11 \Longleftrightarrow 14.400 \equiv 1 \mod 11 \Longleftrightarrow 11|(14.400-1) \Longleftrightarrow 11|(1.309 \times 11)$. Assim, 11 satisfaz a condição (2) e segue-se do Teorema Principal, 11 é um número primo.

***Observação* 4.2** O número 11 é da forma $4k+3$ logo, poderíamos ter substituído diretamente na congruência (8).

5 Comparação entre Teorema de Wilson e o Teorema Principal

Observando as congruências do Teorema de Wilson e do Teorema Principal, equações (1) e (2) respectivamente, podemos observar que o termo à direita de cada uma diferencia os testes de primalidade de ambos teoremas. A parte à esquerda de cada uma é um cálculo imediato de -1 e $(-1)^{\frac{p+1}{2}}$, respectivamente. A partir dessa diferença podemos apresentar alguns resultados.

Proposição 5.1 *Seja $m \in \mathbb{N}^*$, $m > 1$. Se m é ímpar, então $(m-1)! > \left[\left(\frac{m-1}{2}\right)!\right]^2$.*

Demonstração: Na demostração da Proposição 5.1 é uma aplicação imediata da Proposição 2.1, tomando $n = \frac{m-1}{2}$, $m > 1$ e ímpar. □

***Observação* 5.1** Na Proposição 5.1, provamos que para todo primo ímpar p, temos a desigualdade $(p-1)! > \left[\left(\frac{p-1}{2}\right)!\right]^2$, ou seja, em termos de cálculo, o Teorema de Wilson gera números maiores quando comparados com os números gerados pelo Teorema Principal. Porém, fica a dúvida se este "maior"será suficientemente desvantajoso, a tal ponto, que o Teorema Principal seja considerado um teste de primalidade com menor número de operações que as do Teorema de Wilson. Para esclarecer essa dúvida, primeiro, definimos o **Erro** $= \left|\frac{(p-1)!-\left[\left(\frac{p-1}{2}\right)!\right]^2}{(p-1)!}\right|$ e construímos a Tabela 1.

Tabela 1: Teorema de Wilson × Teorema Principal.

p	$(p-1)!$	$\left[\left(\frac{p-1}{2}\right)!\right]^2$	**Erro**
3	2	1	0,5
5	24	4	0,833
7	720	36	0,95
11	3.628.800	14.400	0,996
13	479.001.600	518.400	0,998
17	20.922.789.888.000	1.625.702.400	0,999
⋮	⋮	⋮	⋮

Na Tabela 1, a Coluna 1 apresenta alguns números primos ímpares. A Coluna 2 é aplicação da primeira parte da congruência de (1). A Coluna 3, é aplicação da primeira parte da congruência (2). A Coluna 4, apresenta o Erro, já definido antes.
Observando a Tabela 1 podemos afirmar que quanto maior é o número primo, maior será o Erro e podemos imaginar que tal padrão se mantenha pra primos maiores. De fato, observando os dois teoremas, podemos perceber que a quantidade de fatores presente na expressão do Teorema Principal é metade da quantidade de fatores presente na expressão do Teorema de Wilson.

6 Considerações Finais

As análises apresentadas na Secção 5 corroboram o fato de que o Teorema Principal é mais eficiente que o Teorema de Wilson.

Após a análise deste trabalho podemos concluir que o Teorema Principal (apresentado para os números primos ímpares) é um método alternativo que facilita os cálculos em testes de primalidade de um número.

Infelizmente as duas técnicas de teste de primalidade dados pelo Teorema de Wilson e pelo Teorema Principal tornam-se difíceis de serem executadas para números primos elevados. Em outras palavras, na prática, calcular $k!$ para k elevado é impraticável do ponto de vista computacional.

Enfim, abordar um assunto que não recebe a devida importância nos currículos escolares tanto para alunos quanto para muitos professores foi um grande desafio. A motivação inicial começou quando percebemos o quanto era difícil desvendar os mistérios dos números primos e hoje nos sentimos gratificados pela realização deste trabalho. Espero que como nós, todos os leitores interessados no assunto possam usufruir das informações aqui mostradas e quem sabe possam ser estimulados a desenvolver futuras pesquisas.

7 Agradecimentos

Agradeço primeiramente ao Papai do céu e à Nossa Senhora Aparecida, presenças constantes em minha vida.
Ao apoio do meu marido Wanderson, que me fortaleceu e tranquilizou nos momentos em que mais precisei, mesmo sabendo o quanto era difícil para ele a minha ausência nos momentos de estudos. À minha filha, o perdão pelas diversas vezes que estive ausente nesses dois anos. Ela é a razão disso tudo.
À minha mãe, por nunca ter desistido de mim, por ter sido o alicerce da minha infância e juventude, acreditando sempre que um dia eu daria muito orgulho mesmo no meio de tantas preocupações. À minha sogra Rosely, que me apoiou e ajudou em todos os momentos.
Aos entes queridos que não estão mais presentes e que mandaram muita luz em todos os momentos necessários.
À Prefeitura Municipal de Carandai-MG, juntamente com todos os envolvidos, que permitiram o afastamento do cargo para dedicação desse curso.
Ao meu orientador Prof. Dr. Jorge Andrés Julca Avila, pelo suporte, correções e incentivos.
A toda equipe UFSJ/PROFMAT que ofereceu-me uma oportunidade ímpar de aprimoramento.
As amizades conquistas nesse curso que fizeram uma enorme diferença em cada dia de dificuldade e desespero.
Enfim, a compreensão de todas as pessoas queridas, amigos, familiares, que entenderam que o futuro é feito a partir das escolhas feitas no presente, o meu muito obrigada!

Referências

[1] BOMBIERI, E. Problems of the Millennium: The Riemann Hypothesis. Disponível em: < http://www.claymath.org/sites/default/files/official_problem_description.pdf>. Acesso em: 04 de mar. de 2015.

[2] COUTINHO, Severino. C. Criptografia. 1.ed, Rio de Janeiro, IMPA/OBMEP, 2015.

[3] DOMINGUES, H. H; IEZZI, G. Álgebra Moderna. 4.ed. reform, São Paulo, ATUAL, 2003.

[4] EVEZ, Howard. Introdução à história da matemática, tradução: Hygino H. Domingues. Campinas-SP, UNICAMP, 2004.

[5] HEFEZ, Abramo. Aritmética. 1.ed., Rio de Janeiro, SBM, 2013.

[6] LELLIS, Marcelo. De quem os números primos são primos? Revista de Ensino de Ciências: n. 24, p.20-23, 1993.

[7] LELLIS, Marcelo. O fascínio dos números primos. Revista de Ensino de Ciências: n. 24, p.24-26, 1993.

[8] TASHBULATOVISH, M. M. e RISKULOVICH, E. U. The New Theorem on Prime Number Criterion with Few Operations for the Identification of Prime Number, World Applied Sciences Journal 29 (5): 655-659, 2014.

[9] WIKIPEDIA. John Wilson. Disponível em: <http://www.npg.org.uk/collections/search/portraitLarge/mw195461/Sir-John-Wilson>. Acesso em: 05 dez. 2014.