ReviSeM

Revista Sergipana de Matemática e Educação Matemática

https://doi.org/10.34179/revisem.v9i1.19443

UMA PROVA DA IRRACIONALIDADE DE $\sqrt[2N]{P}$, EM QUE P É PRIMO, POR MEIO DA TEORIA DOS RESÍDUOS QUADRÁTICOS

Renan Jackson Soares Isneri
Universidade Federal de Campina Grande - UFCG
isneri.r.j.s@gmail.com

Vandenberg Lopes Vieira
Universidade Estadual da Paraíba - UEPB
vandenberglv@uepb.edu.br

Maxwell Aires da Silva
Universidade Estadual da Paraíba - UEPB
maxwellaires@servidor.uepb.edu.br

Resumo

Os números primos desempenham um papel fundamental na Teoria dos Números e têm aplicações que vão além da Matemática. Em particular, na Teoria dos Códigos e também na Criptografia, as propriedades dos números primos são relevantes, porque, a partir delas, é possível garantir o armazenamento de dados e o envio de mensagens de forma segura. E isto se evidencia no comércio eletrônico quando dados pessoais devem ser mantidos sob sigilo. A prova de que $\sqrt{p}$ é um número irracional, para todo primo p, é conhecida, se não por todos, mas pela maioria dos estudantes de Matemática, e tal prova é, em geral, dada por meio de uma propriedade básica dos números primos: se p divide o produto de dois inteiros, então, ele divide ao menos um deles. Tal resultado é base de outros não menos importantes, como, por exemplo, o que é dado pelo Teorema Fundamental da Aritmética, que vem a ser o resultado basilar da Teoria dos Números. Neste artigo, apresentamos uma prova da irracionalidade de $\sqrt[2n]{p}$ por meio de resultados da Teoria dos Resíduos Quadráticos, especialmente, pela Lei da Reciprocidade Quadrática de Gauss.

Palavras-chave: Número irracional; Número primo; Resíduo quadrático; Reciprocidade quadrática.

Abstract

Prime numbers play a key role in number theory and have applications beyond Mathematics. In particular, in the Theory of Codes and also in Cryptography, the properties

of prime numbers are relevant, because, from them, it is possible to guarantee the storage of data and the sending of messages in a secure way. And this is evident in e-commerce when personal data must be kept confidential. The proof that $\sqrt{p}$ is an irrational number, for every prime p, is known, if not by everyone, at least by the majority of Mathematics students, and such a proof is, in general, given by means of a basic property of numbers primes: if p divides the product of two integers, then it divides at least one of them. This result forms the basis of other equally important results, such as, for example, what is given by the Fundamental Theorem of Arithmetic, which is the basic result of the Theory of Numbers. In this article, we present a proof of the irrationality of $\sqrt[2n]{p}$ using results from Quadratic Residue Theory, especially, by Gauss's Law of Quadratic Reciprocity.

Keywords: Irrational number; Prime number; Quadratic residue; Quadratic reciprocity.

1 Introdução

O conjunto dos números naturais são os mais familiares dentre os conjuntos numéricos clássicos. Tais números sempre ocuparam e ainda ocupam uma posição de destaque na Teoria dos Números. Segundo [8], ilustres matemáticos se destacaram por estabelecer importantes resultados relacionados a essa teoria. Entre eles, podemos citar Pitágoras (569-500 a.C.), Euclides ($\simeq$ 350 a.C), P. Fermat (1601-1665), L. Euler (1707-1783), A. Legendre (1752-1833), C. Gauss (1777-1855), J. Hadamard (1865-1963), G. H. Hardy (1877-1947).

É importante destacar que esses matemáticos não desenvolviam resultados com a finalidade de que eles um dia viessem a ser aplicados em problemas do cotidiano. A elegância e desafios desses resultados eram suficientes para atraí-los, e isso também é verdade para os atuais estudiosos da área. Atualmente, aplicações em diversas áreas tais como Física, Química, Acústica, Biologia, Computação, Codificação e Criptografia fazem da Teoria dos Números uma área mais atraente, ao menos para os leigos que se deleitam em aplicações da Matemática em problemas do dia a dia.

No conjunto dos números naturais, há a classe dos números primos, que é certamente a mais importante de números inteiros. Isso se deve ao Teorema Fundamental da Aritmética (TFA), o pilar da Teoria dos Números, que afirma o seguinte: *Todo número natural $a > 1$ pode ser escrito, de maneira única exceto pela ordem dos fatores, como um produto de potências de primos.* Em outras palavras, os números primos são suficientes para gerar todos os inteiros diferentes de 0 e ± 1. Isso mostra a importância desses números para a Teoria dos Números. Do ponto de vista de divisibilidade, os primos são

os mais simples, pois os únicos divisores positivos de um primo p são 1 e o próprio p.

A Teoria das Congruências ou Aritmética Modular ocupa uma posição de destaque na Teoria Elementar dos Números, e nela se estuda as propriedades de congruências que são extremamente úteis, pois são uma forte ferramenta de investigação sobre divisibilidade. Por meio de suas propriedades básicas, é possível obter outras mais substanciais, e delas decorrem resultados centrais da Teoria dos Números, como, por exemplo, o Teorema de Fermat e o Teorema de Euler, os quais estabelecem duas importantes congruências. O Teorema de Fermat assegura que, se p é um número primo e a é qualquer inteiro relativamente primo com p, isto é, $\text{mdc}(a, p) = 1$, então,

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.1}$$

Já o Teorema de Euler nos mostra que, se a e m são inteiros, com $\text{mdc}(a, m) = 1$, então,

$$a^{\varphi(m)} \equiv 1 \pmod{m}, \tag{1.2}$$

sendo φ a função de Euler. Nota-se que, quando $m = p$, obtém-se (1.1) a partir de (1.2). Sendo assim, o Teorema de Fermat é um caso particular do Teorema de Euler.

Ainda dentro deste contexto, destaca-se que as propriedades das congruências permitem estudar substancialmente um dos mais notáveis problemas da Teoria Elementar dos Números, a saber, a resolução, em $\mathbb{Z}$, de uma congruência quadrática da forma

$$x^2 \equiv a \pmod{p},$$

em que p é um número primo positivo e a é um inteiro qualquer. Quando existe um inteiro x_0 tal que $x_0^2 \equiv a \pmod{p}$, diz-se que a é um *resíduo ou resto quadrático módulo* p. O estudo de tais números é a essência da Teoria dos Resíduos Quadráticos, e os dois problemas centrais relacionados são os seguintes:

1. Dado um primo p, quais inteiros são resíduos quadráticos de p e quais não são;
2. Dado um inteiro a, determinar os primos p para os quais a é um resíduo quadrático e aqueles para os quais a não é um resíduo quadrático.

O primeiro problema, em princípio, é resolvido por meio do Critério de Euler, embora ele não seja prático para primos relativamente grandes. O segundo é de fato mais difícil, e exigiu quase cinquenta anos de esforços de matemáticos como Euler, Lagrange e Legendre, antes que Gauss apresentasse a primeira solução completa. A solução dos problemas supracitados envolve conceitos e resultados que são clássicos da Teoria dos Resíduos Quadráticos. De um modo geral, a forma mais eficaz de resolvê-los é por meio

da Lei da Reciprocidade Quadrática, uma das grandes contribuições de Gauss à Teoria dos Números. Ela conecta a solubilidade de duas congruências quadráticas,

$$x^2 \equiv p \pmod{q} \quad \text{e} \quad x^2 \equiv q \pmod{p},$$

em que p e q são primos ímpares distintos. É Importante destacar que essa lei já era do conhecimento de Euler e Legendre, mas foi provada por Gauss, provavelmente, sem o conhecimento dos trabalhos de ambos. Gauss, com a idade de 18 anos, no ano de 1795, achava que este resultado era verdadeiro após elaborar uma tabela de 10000 valores para o Símbolo de Legendre (p/q). Contudo, ele só encontrou uma prova depois de um ano, e publicou em seu livro *Disquisitiones Arithmeticae*, no qual apresentou duas demonstrações, sendo uma delas usando Indução Matemática. Porém, constata-se que Gauss apresentou um total de 8 provas distintas da Lei da Reciprocidade Quadrática. Para mais detalhes, veja [2].

O trabalho está organizado da seguinte forma: Na Seção 2, apresentamos definições e resultados básicos relacionados à Teoria dos Resíduos Quadráticos. Antes disto, consideramos as principais propriedades das congruências, de forma que se possa obter resultados mais avançados. A Seção 3 é dedicada às contribuições do nosso trabalho, essencialmente, os resultados dados pelos Teoremas 3.4, 3.5, 3.6 e 3.7. Finalmente, na Seção 4, apresentamos as considerações finais e perspectivas.

2 Definições e Resultados

Destacaremos a seguir os resultados necessários para o desenvolvimento do trabalho. Para mais detalhes sobre o assunto, indicamos as referências [5] e [8]. Nelas, o leitor poderá verificar com mais acuidade os resultados aqui apresentados.

Definição 2.1. Sejam a e b inteiros e m um número natural. Diz-se que a é *congruente* a b *módulo* m quando m divide $a - b$. Em símbolos,

$$a \equiv b \pmod{m} \qquad \text{ou} \qquad a \equiv_m b.$$

A relação de congruência módulo m possui propriedades importantes, e algumas delas semelhantes às da relação de igualdade entre inteiros. Com efeito, de início, ela é uma relação de equivalência sobre $\mathbb{Z}$. O conjunto quociente de $\mathbb{Z}$ por esta relação é, em geral, indicado por $\mathbb{Z}_m$. Por meio do Algoritmo da Divisão, tem-se

$$\mathbb{Z}_m = \{\overline{0},\ \overline{1}, \ldots, \overline{m-1}\},$$

em que $\overline{r} = \{x \in \mathbb{Z} : x \equiv r \pmod{m}\}$. É claro que, se $a \in \mathbb{Z}$ é um múltiplo de m, então, em $\mathbb{Z}_m$, $\overline{a} = \overline{0}$. Ademais, dados a, b, c e d inteiros quaisquer, valem as seguintes propriedades:

1. $a \equiv_m b$ e $c \equiv_m d \Rightarrow \ (a+c) \equiv_m (b+d)$ e $ac \equiv_m bd$.

2. $a \equiv_m b \Rightarrow \ a^k \equiv_m b^k$ qualquer que seja $k \in \mathbb{N}$.

As propriedades reflexiva, simétrica e transitiva da relação $\equiv_m$, juntamente com as três propriedades descritas anteriormente, formam a base da Aritmética Modular. Com elas, pode-se analisar, módulo m, números relativamente grandes, como, por exemplo, estudar módulo 11 o número

$$222^{333} + 333^{222}.$$

Neste caso, verifica-se que $(222^{333} + 333^{222}) \equiv 6 \pmod{11}$.

Definição 2.2. Sejam m e a inteiros, com $m > 1$ e $\text{mdc}(a, m) = 1$. Diz-se que a é um *resíduo* ou *resto quadrático módulo* m (ou de m), quando a congruência quadrática

$$x^2 \equiv a \pmod{m}$$

tem solução inteira, isto é, existe um inteiro x_0 tal que $x_0^2 \equiv a \pmod{m}$. Do contrário, a não é um resíduo quadrático módulo m (ou de m).

Quando a e b são inteiros congruentes módulo p, ou seja, $a \equiv b \pmod{p}$, então, a é um resíduo quadrático de p se, e somente se, b é um resíduo quadrático de p. Dessa forma, visto que $\{0, 1, \ldots, p-1\}$ é um sistema completo de resíduos módulo p, então, para decidir sobre o caráter quadrático de um inteiro qualquer, basta determinar quais inteiros positivos menores do que p são resíduos quadráticos a fim de decidir o mesmo para qualquer outro inteiro.

Exemplo 2.3. Consideremos o primo $p = 11$. Para determinar quais inteiros a, com $1 \leq a \leq 10$, são resíduos quadráticos de $p = 11$, devemos verificar quais congruências $x^2 \equiv a \pmod{11}$ têm soluções. Sob a congruência módulo 11, os quadrados dos inteiros $1, 2, \ldots, 10$ são:

$$1^2 \equiv 10^2 \equiv 1, \quad 2^2 \equiv 9^2 \equiv 4, \quad 3^2 \equiv 8^2 \equiv 9, \quad 4^2 \equiv 7^2 \equiv 5, \quad 5^2 \equiv 6^2 \equiv 3.$$

Portanto, os resíduos quadráticos (incongruentes) de $p = 11$ são 1, 3, 4, 5 e 9, enquanto que os não resíduos quadráticos (incongruentes) são 2, 6, 7, 8 e 10. Para exemplificar o que foi observado sobre inteiros congruentes, observemos o seguinte: uma vez que $1301 \equiv 3 \pmod{11}$ e 3 é um resíduo quadrático de 11, então, 1301 também o é.

Do exemplo anterior, observa-se que a quantidade de resíduos quadráticos (incongruentes) de 11 coincide com a quantidade dos não resíduos quadráticos (incongruentes). Isto se encaixa numa situação geral, dada pelo seguinte teorema:

Teorema 2.4. *Se p é um primo ímpar, então entre os inteiros $1, 2, \ldots, p-1$ existem $(p-1)/2$ resíduos quadráticos e $(p-1)/2$ não resíduos quadráticos de p.*

Uma prova para o teorema anterior pode ser encontrada em [8], no qual a base da prova se baseia no seguinte fato: os resíduos quadráticos de p pertencem às classes de congruências que contêm os quadrados

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Portanto, entre os inteiros $1, 2, \ldots, p-1$, existem $(p-1)/2$ resíduos quadráticos de p, e igual número que não são resíduos quadráticos, pois

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

Vamos indicar por R_p o conjunto dos resíduos quadráticos positivos de p e menores do que p, dois a dois incongruentes módulo p, e por N_p o conjunto dos não resíduos quadráticos positivos de p e menores do que p, também dois a dois incongruentes módulo p. De acordo com o Teorema 2.4, os inteiros de R_p são obtidos reduzindo, módulo p, os inteiros do conjunto

$$R'_p = \left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}.$$

Por exemplo, para $p = 11$, $R'_{11} = \{1^2, 2^2, 3^2, 4^2, 5^2\} = \{1, 4, 9, 16, 25\}$. Logo,

$$R_{11} = \{1, 3, 4, 5, 9\} \quad \text{e} \quad N_{11} = \{2, 6, 7, 8, 10\}.$$

Um fato interessante é que todo inteiro a é um resíduo quadrático de 2, isto é, a congruência $x^2 \equiv a \pmod 2$ tem sempre solução. Por outro lado, para um primo ímpar p qualquer, decidir se um inteiro é ou não um resíduo quadrático é uma tarefa difícil, a menos que se faça uso de resultados clássicos do assunto, como o Critério de Euler e a Lei da Reciprocidade Quadrática. Conforme observamos na Seção 1, os problemas centrais relacionados à Teoria dos Resíduos Quadráticos são os seguintes:

1. Dado um primo p, quais inteiros são resíduos quadráticos de p e quais não são;
2. Dado um inteiro a, determinar os primos p para os quais a é um resíduo quadrático e aqueles para os quais a não é um resíduo quadrático.

Definição 2.5. Sejam p um primo ímpar e a um inteiro qualquer. Define-se o *símbolo de Legendre* $\left(\frac{a}{p}\right)$ ou (a/p) da seguinte forma:

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

É necessário considerar propriedades aritméticas do símbolo de Legendre que possam nos auxiliar a decidir sobre o caráter quadrático de inteiros para primos arbitrários. Nesta direção, o *Critério de Euler*, dado a seguir, nos dá uma caracterização bastante importante.

Teorema 2.6 (Critério de Euler)**.** *Sejam p um primo ímpar e a um inteiro tal que* $\mathrm{mdc}(a, p) = 1$. *Então, a é um resíduo quadrático de p se, e somente se,*

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Para uma prova desse resultado, veja [8].

Exemplo 2.7. Para $a = 2$ e $p = 11$,

$$2^{(11-1)/2} = 2^5 \equiv -1 \pmod{11}.$$

Portanto, 2 não é um resíduo quadrático de $p = 11$. Por outro lado, para $a = 14$ e $p = 1553$,

$$14^{(1553-1)/2} = 14^{776},$$

um número com 890 dígitos e, de fato, é bastante trabalhoso decidir se

$$14^{776} \equiv 1 \pmod{1553} \quad \text{ou} \quad 14^{776} \not\equiv 1 \pmod{1553}.$$

O Exemplo anterior mostra que o Critério de Euler não é tão eficiente quando consideramos primos relativamente grandes. Por isso, faz-se necessário considerar outras técnicas mais eficientes.

Teorema 2.8. *Sejam p um primo ímpar e a e b inteiros quaisquer. Então, o símbolo de Legendre tem as seguintes propriedades:*

(1) Se $a \equiv b \pmod{p}$, *então* $(a/p) = (b/p)$.

(2) $(a^2/p) = 1$, *desde que* $p \nmid a$.

(3) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$.

(4) $(-1/p) = (-1)^{(p-1)/2}$.

(5) $(ab/p) = (a/p)\,(b/p)$, *ou seja, o símbolo de Legendre é uma função totalmente multiplicativa.*

Em [5], há uma prova, usando apenas o Critério de Euler, de uma caracterização dos primos para os quais 2 é um resíduo quadrático; é o seguinte: se p é um primo ímpar, então,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se} \quad p \equiv 1 \pmod{8} \quad \text{ou} \quad p \equiv 7 \pmod{8}, \\ -1 & \text{se} \quad p \equiv 3 \pmod{8} \quad \text{ou} \quad p \equiv 5 \pmod{8}. \end{cases} \tag{2.1}$$

Este é um exemplo de caracterização mais simples de ser resolvido sem o auxílio da Lei da Reciprocidade Quadrática. Conforme destacamos, esse problema foi totalmente resolvido por meio dessa lei.

Teorema 2.9 (Lei da Reciprocidade Quadrática)**.** *Se p e q são números primos ímpares distintos, então*

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

Vamos agora à função de Euler, uma das mais importantes funções aritméticas.

Definição 2.10. Para cada inteiro $n \geq 1$, indiquemos por $\varphi(n)$ o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n. A função assim definida é chamada *função φ de Euler*.

Em particular, $\varphi(8) = 4$, pois os únicos números naturais menores do que ou iguais a 8 que são relativamente primos com 8 são: 1, 3, 5 e 7. Se p é primo e k é um inteiro tal que $k \geq 1$,

$$\varphi(p^k) = p^k - p^{k-1}.$$

Mais ainda, se m e n são números naturais, com $\text{mdc}(m, n) = 1$,

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

Por esta razão, se $n > 1$ e $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ é a fatoração canônica de n, então, por meio de indução sobre r, obtemos

$$\varphi(n) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_r^{k_r} - p_r^{k_r-1}\right).$$

Por exemplo, como $1008 = 2^4 \cdot 3^2 \cdot 7$, tem-se:

$$\varphi(1008) = \varphi(2^4)\varphi(3^2)\varphi(7) = (2^4 - 2^3)(3^2 - 3)(7 - 1) = 288.$$

O Teorema de Dirichlet, em honra ao matemático alemão J. P. G. Lejeune Dirichlet (1805-1859), é um resultado central na Teoria dos Números e tem diversas aplicações em diferentes ramos da Matemática, como, por exemplo, na Teoria Analítica dos Números. Este teorema fornece um resultado importante sobre a distribuição dos números primos, e assegura que existem infinitos deles com determinados padrões aritméticos; isto vai de encontro à percepção de que os números primos se tornam cada vez mais escassos à medida que os números aumentam. O Teorema de Dirichlet tem uma prova relativamente difícil e, por isso, não será aqui apresentada. Para este fim, recomendamos a referência [4],

Teorema 2.11 (Dirichlet)**.** *Sejam a e b inteiros tais que $mdc(a, b) = 1$. Então existem infinitos primos da forma $ak + b$, em que k é inteiro.*

O resultado de Dirichlet diz não somente que existe um número primo da forma $ak + b$ para algum $k \in \mathbb{Z}$, mas também que se considerarmos casos particulares de inteiros a e b tais que $\text{mdc}(a, b) = 1$, então, a progressão aritmética $ak + b$, $k \in \mathbb{Z}$, terá uma infinidade de primos. Por exemplo, para os inteiros $a = 4$ e $b = 3$, primos entre si, existem infinitos números primos da forma $4k + 3$ com $k \in \mathbb{Z}$.

3 Resultados Principais

Nesta seção, apresentaremos as contribuições do nosso trabalho, dadas nos Teoremas 3.4, 3.5, 3.6 e 3.7. Começamos pelo seguinte lema, que é uma consequência da Lei da Reciprocidade Quadrática cuja demonstração pode ser encontrada em [1, 8].

Lema 3.1. *Se p e q são primos ímpares distintos, então*

$$q \in R_p \quad \Leftrightarrow \quad (-1)^{(p-1)/2} \cdot p \in R_q.$$

Lema 3.2. *Sejam $q > 2$ um número primo e $b \in \mathbb{Z}$ tal que $(b/q) = 1$ e $b \equiv 1 \pmod 4$. Então, existe um inteiro ímpar $a \in \{1, 3, \ldots, q - 2\}$, com $b \equiv a^2 \pmod{4q}$.*

Demonstração. Como $(b/q) = 1$, a congruência quadrática

$$x^2 \equiv b \pmod q \tag{3.1}$$

tem uma solução $x_0 = a$ em $\mathbb{Z}$. Sem perda de generalidade podemos assumir que $a \in \{1, 2, \ldots, q-1\}$. Com efeito, pelo Algoritmo da Divisão, existe um inteiro r tal que $r \in \{1, 2, \ldots, q-1\}$ e $r \equiv a \pmod{q}$ e, então, r também é solução de (3.1), o que justifica a escolha de a. Ademais, é claro que $q - a$ também é solução de (3.1) e, desde que q é ímpar, a e $q-a$ têm paridades diferentes com $q-a \in \{1, 2, \ldots, q-1\}$. Portanto, sem perda de generalidade, suponhamos que a é ímpar com $a \in \{1, 3, ..., q-2\}$ e, assim, $a^2 \equiv 1 \pmod{4}$. Por outro lado, o fato $b \equiv 1 \pmod{4}$ implica $b \equiv a^2 \pmod{4}$. Portanto,

$$q \mid b - a^2 \quad \text{e} \quad 4 \mid b - a^2.$$

Desse modo, $b \equiv a^2 \pmod{4q}$, pois $\text{mdc}(4, q) = 1$. □

O resultado a seguir nos dá um critério sobre o caráter quadrático entre dois primos ímpares distintos.

Teorema 3.3. *Sejam q e p primos ímpares distintos. Então, as seguintes afirmações são equivalentes:*

(1) *q é um resíduo quadrático módulo p.*

(2) *Existe um inteiro ímpar $a \in \{1, 3, \ldots, q-2\}$ tal que*

$$p \equiv a^2 \pmod{4q} \quad \textit{ou} \quad p \equiv -a^2 \pmod{4q}.$$

Demonstração. Suponhamos q um resíduo quadrático de p, isto é, $(q/p) = 1$. Assim, pelo Lema 3.1,

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

Agora, se $p \equiv 1 \pmod{4}$ ou $p \equiv 3 \pmod{4}$, então $(-1)^{(p-1)/2}p \equiv 1 \pmod{4}$. De fato, $p \equiv 1 \pmod{4}$ implica $(-1)^{(p-1)/2}p \equiv p \equiv 1 \pmod{4}$. Por outro lado, se $p \equiv 3 \pmod{4}$,

$$(-1)^{(p-1)/2}p \equiv -p \equiv -3 \equiv 1 \pmod{4}.$$

Por isso, em ambos os casos, $(-1)^{(p-1)/2}p \equiv 1 \pmod{4}$. Desse modo, pelo Lema 3.2, existe um inteiro ímpar $a \in \{1, 3, \ldots, q-2\}$ tal que

$$(-1)^{(p-1)/2}p \equiv a^2 \pmod{4q}.$$

Portanto,

$$p \equiv a^2 \pmod{4q} \quad \text{ou} \quad p \equiv -a^2 \pmod{4q}.$$

Reciprocamente, existe um inteiro ímpar $a \in \{1, 3, \ldots, q-2\}$, com

$$p \equiv a^2 (\mathrm{mod}\, 4q) \quad \text{ou} \quad p \equiv -a^2 \,(\mathrm{mod}\, 4q).$$

Sendo $p \equiv a^2 \,(\mathrm{mod}\, 4q)$, então, em particular, $p \equiv a^2 \ (\mathrm{mod}\, 4)$. Visto que, para todo inteiro ímpar a, $a^2 \equiv 1 \,(\mathrm{mod}\, 4)$, obtemos $p \equiv 1 \,(\mathrm{mod}\, 4)$. Agora, pela Lei da Reciprocidade Quadrática,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1. \tag{3.2}$$

Como $p \equiv a^2 \,(\mathrm{mod}\, 4q)$, tem-se $p \equiv a^2 \,(\mathrm{mod}\, q)$ e, daí, $(p/q) = 1$. Por (3.2), obtém-se $(q/p) = 1$. Agora, o fato $p \equiv -a^2 \,(\mathrm{mod}\, 4q)$ implica $p \equiv 3 \,(\mathrm{mod}\, 4)$, pois $-p \equiv a^2 \,(\mathrm{mod}\, 4)$ e $a^2 \equiv 1 \,(\mathrm{mod}\, 4)$. Dessa maneira,

$$\left(\frac{-p}{q}\right) = 1 \quad \text{e} \quad \left(\frac{-1}{p}\right) = -1.$$

Ainda pela Lei da Reciprocidade Quadrática,

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

Multiplicando a igualdade anterior por $(-1/q)$,

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

ou melhor,

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

Uma vez que $(-1/q) = (-1)^{(q-1)/2}$, $(-1/p) = (-1)^{(p-1)/2} = -1$ e $(-p/q) = 1$, temos

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}}(-1)^{\frac{q-1}{2}}. \tag{3.3}$$

Logo, $(q/p) = 1$. Portanto, em ambos os casos, q é um resíduo quadrático de p. □

Teorema 3.4. *Se p é um primo ímpar, então existe um primo $q > 2$, $p \neq q$, tal que*

$$\left(\frac{p}{q}\right) = -1. \tag{3.4}$$

Demonstração. Primeiramente, afirmamos que existe um inteiro b tal que $0 < b < 4p$, $\text{mdc}(b, 4p) = 1$ e

$$b \not\equiv a^2 \,(\text{mod}\, 4p) \quad \text{e} \quad b \not\equiv -a^2 \,(\text{mod}\, 4p), \quad \forall a \in A,$$

em que $A = \{1, 3, \ldots, p-2\}$. Com efeito, notemos inicialmente que

$$\varphi(4p) = \varphi(4)\varphi(p) = 2(p-1),$$

de onde segue que existem $2(p-1)$ inteiros entre os números $1, 2, \ldots, 4p$ que são relativamente primos com $4p$. Por outro lado, como $a^2 \not\equiv -a^2 \,(\text{mod}\, 4p)$ para todo $a \in A$, deduzimos que o conjunto $A^2 = \{a^2, -a^2 \mid a \in A\}$ possui exatamente $p-1$ elementos, digamos

$$A^2 = \{a_1, a_2, \ldots, a_{p-2}, a_{p-1}\}.$$

Consequentemente, pelo Algoritmo da Divisão, para cada $i = 1, 2, \ldots, p-1$, existe um inteiro r_i verificando $0 < r_i < 4p$ e

$$r_i \equiv a_i \,(\text{mod}\, 4p).$$

Desse modo, podemos escolher um inteiro b entre os números $1, \ldots, 4p-1$ tais que $\text{mdc}(b, 4p) = 1$ e $b \neq r_i$ para todo $i = 1, 2, \ldots, p-1$ e, portanto, b satisfaz nossa afirmação. De fato, se existe $a \in A$ satisfazendo $b \equiv a^2 \,(\text{mod}\, 4p)$ ou $b \equiv -a^2 \,(\text{mod}\, 4p)$, então devemos ter $b \equiv r_i \,(\text{mod}\, 4p)$ para algum i e, assim, $4p$ divide $b - r_i$. No entanto, como $0 < b, r_i < 4p$ concluímos que $b = r_i$, um absurdo. Por fim, invocando o Teorema 2.11, existe $k_0 \in \mathbb{Z}$ tal que $q = (4p)k_0 + b$ é um número primo. Logo, $q \equiv b \,(\text{mod}\, 4p)$ e, por conseguinte,

$$q \not\equiv a^2 \,(\text{mod}\, 4p) \quad \text{e} \quad q \not\equiv -a^2 \,(\text{mod}\, 4p), \quad \forall a \in A.$$

De acordo com o Teorema 3.3, q não é um resíduo quadrático módulo p, ou seja,

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

Isto finalmente conclui a prova. □

Similarmente, pode-se provar o seguinte teorema.

Teorema 3.5. *Se p é um primo ímpar, então existe um primo $q > 2$, $p \neq q$, tal que*

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

Talvez a prova de que o número real $\sqrt{2}$ é irracional seja a primeira a ser apresentada para os alunos iniciantes de matemática. Para Pitágoras, um matemático grego da cidade de Samos, os números racionais eram "completos", no sentido de eles explicarem todos os fenômenos naturais. Em [6], relata-se que um dos alunos de Pitágoras, chamado Hipaso, chegou à conclusão de que $\sqrt{2}$ não poderia ser escrito como uma fração de dois números inteiros. Tal fato o levou à morte, pois a ideia de irracionalidade não era aceita, sob nenhuma hipótese.

Euclides, um matemático grego de Alexandria, foi o primeiro a provar a irracionalidade de $\sqrt{2}$. A demonstração dada por ele, feita por *reductio ad absurdum*, está entre as mais notáveis de toda a Matemática. Essa prova se encontra no clássico livro *Os Elementos*[1] de sua autoria. Desde então, os números irracionais passaram a ter um tratamento à parte. Há várias provas para a irracionalidade de $\sqrt{2}$, todas baseadas em resultados básicos da Teoria Elementar dos Números, como, por exemplo, por meio do Teorema Fundamental da Aritmética, do Princípio da Boa Ordenação (PBO) e por Frações Contínuas, [7]. O mesmo princípio utilizado por Euclides pode ser usado a fim de provar que $\sqrt{p}$ é irracional qualquer que seja o primo positivo p. No teorema seguinte, apresentamos uma prova por meio de resíduos quadráticos.

Teorema 3.6. *Se p é um primo ímpar, então $\sqrt{p}$ é irracional.*

Demonstração. Suponhamos, por absurdo, $\sqrt{p}$ um número racional. Assim, existem a e b inteiros tais que

$$pb^2 = a^2,$$

em que $b \neq 0$. À luz do Teorema 3.4, tomemos um primo ímpar q tal que p não é um resíduo quadrático de q, isto é, $(p/q) = -1$. Agora, como as congruências

$$x^2 \equiv a^2 \pmod{q} \quad \text{e} \quad x^2 \equiv b^2 \pmod{q}$$

têm solução,

$$\left(\frac{a^2}{q}\right) = \left(\frac{b^2}{q}\right) = 1.$$

[1]Essa obra consiste no livro matemático mais bem-sucedido já escrito. Com mais de mil edições, ele é composto de treze volumes, fornecendo uma introdução à Geometria Plana e à Geometria Sólida, bem como à Teoria dos Números. Por exemplo, algumas propriedades da paridade de inteiros são dadas nas Proposições 21-29 do volume IX. O Algoritmo de Euclides para calcular o máximo divisor comum de dois inteiros positivos é encontrado no volume VII nas Proposições 2 e 3, respectivamente; e suas provas para a infinitude dos números primos e uma condição suficiente para que números pares sejam perfeitos são encontradas no volume IX em suas Proposições 20 e 36, respectivamente.

De acordo com o item (5) do Teorema 2.8, o símbolo de Legendre é uma função totalmente multiplicativa. Assim,

$$1 = \left(\frac{a^2}{q}\right) = \left(\frac{pb^2}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{b^2}{q}\right) = \left(\frac{p}{q}\right),$$

uma contradição, pois $(p/q) = -1$. Portanto, $\sqrt{p}$ é irracional. □

Mais geralmente, usando argumento semelhante ao da prova do Teorema 3.6, provaremos o seguinte resultado:

Teorema 3.7. *Se p é um primo ímpar, então, $\sqrt[2n]{p}$ é um número irracional para todo inteiro positivo n.*

Demonstração. Suponhamos $\sqrt[2n]{p}$ um número racional. Logo, por definição, existem inteiros positivos a e b tais que $\sqrt[2n]{p} = a/b$, ou melhor,

$$pb^{2n} = a^{2n}. \tag{3.5}$$

Pelo Teorema 3.4, existe um primo $q > 2$ satisfazendo $(p/q) = -1$. Por outro lado, $x_0 = a^n$ e $x_0' = b^n$ são, respectivamente, soluções das congruências quadráticas

$$x^2 \equiv a^{2n} \pmod{q} \quad \text{e} \quad x^2 \equiv b^{2n} \pmod{q}.$$

Portanto,

$$\left(\frac{a^{2n}}{q}\right) = \left(\frac{b^{2n}}{q}\right) = 1. \tag{3.6}$$

Assim, combinando (3.5) com (3.6), obtém-se

$$1 = \left(\frac{a^{2n}}{q}\right) = \left(\frac{pb^{2n}}{q}\right) = \left(\frac{p}{q}\right),$$

o que contradiz a escolha do primo q. □

4 Conclusões Finais e Perspectivas

A Teoria dos Resíduos Quadráticos, um ramo da Teoria dos Números, possui resultados substanciais com aplicações importantes, por exemplo, na busca de algoritmos para fatoração de números inteiros, na construção de bons códigos e no estudo de curvas elípticas e, neste último caso, se aplica a corpos finitos, que são fundamentais em criptografia moderna. Em nosso caso, consideramos uma das principais contribuições

de Gauss à Teoria dos Números, a Lei da Reciprocidade Quadrática, com a finalidade de provar a irracionalidade de números da forma $\sqrt[2n]{p}$, sendo p um número primo e n um inteiro positivo qualquer.

Embora o Teorema 3.7 seja considerado para números primos ímpares, não existe restrição para $p = 2$. Neste caso, para provar que $\sqrt{2}$ é irracional usando o argumento do Teorema 3.7, basta usar a caracterização dos primos p para os quais 2 é um resíduo quadrático ou não de p dada em (2.1). Caracterizações como esta são estabelecidas para cada número primo p e isso decorre do Teorema 3.3, porém, à medida que o valor de p cresce, isto se torna uma tarefa árdua. O leitor interessado pode ver [3] para uma discussão detalhada sobre este tópico.

É natural se questionar sobre uma prova para a irracionalidade de $\sqrt[2n+1]{p}$ por meio dos argumentos usados neste trabalho. No entanto, neste caso, o procedimento em questão não é mais válido. Com efeito, suponhamos que exitam inteiros a e b tais que $b \neq 0$ e $\sqrt[2n+1]{p} = a/b$, de onde segue que $pb^{2n+1} = a^{2n+1}$. Agora, desde que

$$\left(\frac{b^{2n+1}}{q}\right) = \left(\frac{b}{q}\right) \quad \text{e} \quad \left(\frac{a^{2n+1}}{q}\right) = \left(\frac{a}{q}\right)$$

para qualquer número primo q, então para aplicar nosso argumento é necessário conhecer o caráter quadrático de a e b módulo q, o que é uma tarefa difícil.

Referências

[1] Buck, Nancy.; *Quadratic Reciprocity for the Rational Integers and the Gaussian Integers*. Thesis (Master of Arts) - University of North Carolina at Greensboro, 2010, 80 pp.

[2] Burton, David M.; *Elementary Number Theory*. Allyn and Bacon, Inc., University of New Hampshire, Boston, 1980.

[3] Isneri, Renan J. S.; *Resíduos Quadráticos*. Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Campina Grande, 2017, 81 pp.

[4] Martinez, Fabio B. et al.; *Teoria dos Números*: um passeio com primos e outros números familiares pelo mundo inteiro (2ª edição). IMPA, Projeto Euclides, Rio de Janeiro, 2011.

[5] Santos, José Plínio O.; *Introdução à Teoria dos Números*. 3ª edição, IMPA, Rio de Janeiro, 2009.

[6] Singh, Simon.; *O Último Teorema de Fermat*. 13ª edição, Editora Record Ltda, Rio de Janeiro, 2012.

[7] Oliveira, Gilberto A.; *Números Irracionais e Transcendentes*. Dissertação (PROFMAT) - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto, 2015, 86 pp.

[8] Vieira, Vandenberg L.; *Um Curso Básico em Teoria dos Números*, 2ª edição, Editora Livraria da Física, São Paulo, 2020.

Recebido em 26 de Julho de 2023.
1ª Revisão em 27 de Setembro de 2023.
Aceito em 14 de Novembro de 2023.