

**PROGRAMA DE
PÓS-GRADUAÇÃO EM
MATEMÁTICA**

**Reciprocidade Quadrática e Algumas Aplicações
com o Uso do Software SageMath**

Danilo Alves Rodrigues

INSTITUTO DE GEOCIÊNCIAS E CIÊNCIAS EXATAS

RIO CLARO
2025

UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Danilo Alves Rodrigues

Reciprocidade Quadrática e Algumas Aplicações com o Uso do Software SageMath

Dissertação de Mestrado apresentada ao Instituto de Geociências e Ciências Exatas do Câmpus de Rio Claro, da Universidade Estadual Paulista “Júlio de Mesquita Filho”, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Orientadora
Profa. Dra. Carina Alves

**Rio Claro/SP
2025**

R696r Rodrigues, Danilo Alves
Reciprocidade quadrática e algumas aplicações com o uso do
software SageMath / Danilo Alves Rodrigues. -- Rio Claro, 2025
80 p.

Dissertação (mestrado profissional) - Universidade Estadual
Paulista (UNESP), Instituto de Geociências e Ciências Exatas, Rio
Claro
Orientador: Carina Alves

1. Álgebra. 2. Congruências lineares. 3. Resíduos quadráticos. 4.
Reciprocidade quadrática. I. Título.

Impacto potencial desta pesquisa

Esta pesquisa tem como objetivo principal fornecer um material didático para estudantes da área da matemática e áreas afins, apresentando de forma clara e acessível conceitos fundamentais da aritmética modular e suas aplicações em áreas práticas. Os exemplos detalhados e as explicações teóricas proporcionam uma base sólida para estudantes que precisam estudar teoria dos números, além de incentivar a exploração de algumas aplicações, como a criptografia e a teoria dos códigos, que são cada vez mais relevantes em um mundo altamente digitalizado. Além disso, professores podem utilizar este trabalho como referência tanto para o ensino quanto para o desenvolvimento de novas aplicações, como a utilização da Lei da Reciprocidade Quadrática em teoria dos códigos cíclicos, promovendo colaborações interdisciplinares.

Potential impact of this research

This research aims to provide didactic material for students in the field of mathematics and related areas, presenting fundamental concepts of modular arithmetic and its applications in practical fields in a clear and accessible manner. The detailed examples and theoretical explanations offer a solid foundation for students who need to study number theory, while also encouraging the exploration of certain applications, such as cryptography and coding theory, which are increasingly relevant in a highly digitalized world. Additionally, teachers can use this work as a reference both for teaching and for the development of new applications, such as the use of the Quadratic Reciprocity Law in the theory of cyclic codes, promoting interdisciplinary collaborations.

UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Danilo Alves Rodrigues

RECIPROCIDADE QUADRÁTICA E ALGUMAS APLICAÇÕES COM O USO DO
SOFTWARE SAGEMATH

Dissertação de Mestrado apresentada ao Instituto de Geociências e Ciências Exatas do Câmpus de Rio Claro, da Universidade Estadual Paulista “Júlio de Mesquita Filho”, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Comissão Examinadora

Profa. Dra. Carina Alves
IGCE / UNESP / Rio Claro (SP)

Profa. Dra. Suzete Maria Silva Afonso
IGCE / UNESP / Rio Claro (SP)

Profa. Dra. Grasielle Cristiane Jorge
ICT / UNIFESP / São José dos Campos (SP)

Conceito: Aprovado

Rio Claro (SP), 09 de abril de 2025

Dedico este trabalho a todos que me impulsionaram, seja por apoio ou por obstáculos. Cada um deles me transformou e me fortaleceu para alcançar este objetivo.

Agradecimentos

Gostaria de expressar minha profunda gratidão a todos que tornaram esta dissertação possível.

Primeiramente, agradeço aos meus pais, Cibele e Milton, e ao meu irmão, Dênis, por todo o apoio dedicado.

Aos meus amigos, Cássio, Douglas, Felipe e Rafael. Sua amizade, compreensão e apoio nos momentos bons e nos mais turbulentos me ajudaram a seguir em frente com mais ânimo e alegria.

Aos professores do PGMAT, que compartilharam seus conhecimentos com generosidade e me inspiraram a buscar sempre mais. Agradeço também aos meus colegas de curso, pelas conversas, debates e aprendizado mútuo.

Um agradecimento especial ao "Grupo do Choro", Angelita, Andreza, Enio, Francisco, Gabriela, Kadu, Margarete e Sara. Suas presenças constantes, apoio emocional e incentivo foram essenciais para minha trajetória. As risadas, os choros e o companheirismo de vocês tornaram essa jornada possível.

Finalmente, gostaria de expressar minha imensa gratidão à minha orientadora, Professora Doutora Carina Alves. Sua orientação, sabedoria, paciência e dedicação foram fundamentais para a realização desta dissertação. Agradeço por sua confiança em mim, por seus ensinamentos valiosos e por me guiar com tanta maestria.

Tente mover o mundo, o primeiro passo será mover a si mesmo.

Platão

Resumo

Esta dissertação aborda conceitos fundamentais da teoria dos números, com foco em congruências lineares, resíduos quadráticos e, especialmente, na Lei da Reciprocidade Quadrática. No trabalho, são apresentadas três diferentes demonstrações para a Lei da Reciprocidade Quadrática: a primeira utilizando o lema de Eisenstein, a segunda baseada em raízes da unidade e a terceira empregando a teoria dos grupos. Essas abordagens proporcionam uma visão abrangente da reciprocidade quadrática e suas diversas perspectivas teóricas. Além disso, a dissertação explora aplicações desses conceitos em áreas como criptografia, teoria dos grafos e teoria dos códigos, demonstrando a relevância prática da teoria dos números. Exemplos incluem a aplicação da reciprocidade quadrática no Sistema Criptográfico de Rabin e em códigos cíclicos, com algumas implementações feitas no software livre *SageMath*.

Palavras-chave: Álgebra. Congruências Lineares. Resíduos Quadráticos. Reciprocidade Quadrática.

Abstract

This dissertation addresses fundamental concepts of number theory, focusing on linear congruences, quadratic residues, and especially the Quadratic Reciprocity Law. The work presents three different proofs of the Quadratic Reciprocity Law: the first using Eisenstein's lemma, the second based on roots of unity, and the third employing group theory. These approaches provide a comprehensive view of quadratic reciprocity and its various theoretical perspectives. Additionally, the dissertation explores applications of these concepts in areas such as cryptography, graph theory, and coding theory, demonstrating the practical relevance of number theory. Examples include the application of quadratic reciprocity in the Rabin Cryptosystem and cyclic codes, with some implementations made in the free software *SageMath*.

Keywords: Algebra. Linear Congruences. Quadratic Residues. Quadratic Reciprocity.

Lista de Figuras

5.1	Grafo de Paley P_5 com $q = 5$. Fonte: Elaborada pelo autor no Sagemath.	70
-----	---	----

Sumário

1	Introdução	13
2	Congruências Lineares	15
2.1	Aritmética dos Restos	15
2.2	Cr�terios de divisibilidade via congru�ncia	20
2.3	Congru�ncias Lineares	21
2.4	Teorema Chin�s dos Resto	28
3	Res�duos Quadr�ticos e Congru�ncias Quadr�ticas	31
3.1	Res�duos Quadr�ticos	31
3.2	S�mbolo de Legendre	39
4	Provas da Lei da Reciprocidade Quadr�tica	45
4.1	Primeira prova: Usando o lema de Eisenstein	46
4.2	Segunda prova: Usando ra�zes da unidade	49
4.3	Terceira prova: Usando Teoria dos Grupos	53
5	Aplica��es	56
5.1	Lei da Reciprocidade Quadr�tica em Criptografia	56
5.1.1	Aplica��o 1: Teste de Miller–Rabin	57
5.1.2	Exemplo usando Sagemath	60
5.1.3	Aplica��o 2: Sistema Criptogr�fico de Rabin.	61
5.1.4	Exemplo usando SageMath	64
5.1.5	Aplica��o 3: Teste de Primalidade de Solovay-Strassen	66
5.1.6	Exemplo usando Sagemath	67
5.2	Lei da Reciprocidade Quadr�tica em Teoria dos Grafos	68
5.2.1	Aplica��o: Grafos de Paley	68
5.2.2	Exemplo usando Sagemath	70
5.3	Lei da Reciprocidade Quadr�tica em Teoria dos C�digos	70
5.3.1	Aplica��o: Teoria dos C�digos C�clicos	71
5.3.2	Exemplo usando Sagemath	72

6	Considerações Finais	74
	Referências	75

1 Introdução

A Teoria dos Números, um dos campos mais antigos e fundamentais da matemática, tem sido estudada por muitos séculos, com contribuições de notáveis matemáticos que moldaram o entendimento moderno dessa área. Entre os tópicos mais importantes dentro dessa teoria está a Lei da Reciprocidade Quadrática, considerada por Carl Friedrich Gauss como o “Teorema Áureo” ou o “Teorema Fundamental”. Esse teorema, que fornece uma maneira de determinar se uma congruência do tipo $x^2 \equiv a \pmod{p}$ tem solução.

A Lei da Reciprocidade Quadrática passou por várias formulações e tentativas de demonstração ao longo dos séculos XVIII e XIX. O primeiro a conjecturá-la foi o matemático suíço Leonhard Euler no século XVIII, que forneceu uma resposta correta, mas sem uma prova rigorosa. Mais tarde, Adrien-Marie Legendre formalizou a conjectura em 1785, denominando-a como "Lei da Reciprocidade Quadrática", mas suas tentativas de prova continham falhas. Foi apenas com Carl Friedrich Gauss, em 1795, que a primeira demonstração rigorosa foi apresentada, quando Gauss tinha apenas 18 anos. Gauss continuou trabalhando neste teorema durante toda a sua vida, e ao longo de suas publicações e notas póstumas, revelou-se um total de oito provas diferentes para o teorema. Gauss acreditava que encontrar diferentes abordagens para a demonstração do teorema poderia permitir a sua generalização para estudos mais elevados, o que abriu caminho para o desenvolvimento de partes significativas da teoria algébrica dos números.

A importância desta lei vem de ser um dos pilares da teoria dos números moderna, além de ter conexão com outras áreas da matemática, como aplicações na teoria dos números algébricos, a geometria algébrica e a teoria dos números p-ádicos, e em outras ciências, como a Física e a Ciência da Computação, além de ser um tema instigante, onde sempre há buscas por novas demonstrações e generalizações do teorema.

Se houver interesse, o livro *Reciprocity Laws: From Euler to Eisenstein* [1], apresenta diversas demonstrações da lei da reciprocidade quadrática em diferentes áreas da matemática, sendo uma excelente fonte de referência para aprofundamento nesta lei onde há dezenas de demonstrações.

Esta dissertação se dedica a explorar como a Lei da Reciprocidade Quadrática se manifesta em diversas áreas, desde a segurança de sistemas criptográficos como o de Rabin [2], passando por testes de primalidade como o de Solovay-Strassen [3] e o de Miller-Rabin [4], até a aplicação em problemas relacionados à teoria dos grafos [5].

O objetivo desta dissertação é apresentar uma visão abrangente sobre a Lei da Reciprocidade Quadrática, explorando três demonstrações distintas: uma baseada no lema de Eisenstein, outra usando raízes da unidade, e a terceira empregando a teoria dos grupos. Essas abordagens não apenas elucidam a riqueza teórica do teorema, mas também destacam sua versatilidade e a importância de sua compreensão a partir de diferentes perspectivas matemáticas.

No Capítulo 2, apresentamos resultados sobre congruências e congruências lineares, sendo que o principal resultado abordado e que finaliza o capítulo é o Teorema Chinês do Resto (TCR). O TCR oferece uma maneira eficaz de resolver sistemas de equações congruentes de módulos diferentes. Se temos um sistema de congruências com módulos primos entre si, o teorema garante a existência de uma solução única módulo o produto desses módulos e isso facilita a resolução de problemas que envolvem divisões em diferentes bases ou corpos de números.

No Capítulo 3, abordamos resíduos quadráticos e conceitos que serão usados no capítulo seguinte, sendo que os principais são o critério de Euler e a definição de símbolo de Legendre.

No Capítulo 4, apresentamos três provas distintas para a Lei da Reciprocidade Quadrática, cada uma utilizando técnicas variadas que exploram aspectos diferentes da matemática. Essas abordagens demonstram a flexibilidade da lei ao ser tratada por métodos variados, desde aritméticos até algébricos. A primeira prova apresentada baseia-se no lema de Eisenstein, uma técnica que envolve a contagem de pontos de reticulados, oferecendo uma maneira geométrica de abordar o problema. A segunda prova faz uso de raízes da unidade, destacando a conexão da reciprocidade quadrática com a teoria dos números algébricos e a aritmética modular. Por fim, a terceira prova utiliza teoria dos grupos, demonstrando como a estrutura algébrica pode ser aplicada para abordar de forma mais moderna e geral a lei.

No capítulo 5, verificamos as aplicações da reciprocidade quadrática, como na criptografia, teoria dos grafos e teoria dos códigos, além de utilizar o software livre *SageMath* [6, 7] em alguns exemplos, demonstrando assim, uma forma de sua utilização atual.

2 Congruências Lineares

O estudo das congruências é um dos pilares fundamentais da teoria dos números, com aplicações que vão desde a criptografia até a resolução de problemas aritméticos clássicos. Ao longo deste capítulo, a noção de congruências e suas características fundamentais serão exploradas sistematicamente, começando com uma visão geral da aritmética dos restos e critérios de divisibilidade por meio de congruências, que oferecem instrumentos significativos para determinar divisibilidades de maneira direta e eficiente. Posteriormente, as congruências lineares, que ocupam uma posição crucial na resolução de equações modulares, serão elucidadas. Também provamos o Teorema de Wilson, que fornece critérios para estabelecer se um número é primo ou não, culminando em uma discussão sobre o Teorema Chinês do Resto, um dos resultados mais elegantes e úteis, com amplas aplicações tanto teóricas quanto práticas. As principais referências usadas para o desenvolvimento deste capítulo foram [8, 9, 10, 11, 12].

2.1 Aritmética dos Restos

Definição 2.1. Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m , escreve-se

$$a \equiv b \pmod{m}.$$

Quando a relação $a \equiv b \pmod{m}$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m . Escreveremos, nesse caso, $a \not\equiv b \pmod{m}$.

Exemplo 2.2. Por exemplo, $21 \equiv 13 \pmod{2}$, já que os restos da divisão de 21 e de 13 por 2 são iguais a 1.

Como o resto da divisão de um número inteiro qualquer por 1 é sempre nulo, temos que $a \equiv b \pmod{1}$, quaisquer que sejam $a, b \in \mathbb{Z}$. Isso torna desinteressante a aritmética dos restos módulo 1. Portanto, doravante, consideraremos sempre $m > 1$.

Decorre, imediatamente, da Definição 2.1 que a congruência, módulo um inteiro positivo fixado m , é uma relação de equivalência. Vamos enunciar isso explicitamente abaixo.

Proposição 2.3. *Seja $m \in \mathbb{Z}$, com $m > 1$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que*

- (i) $a \equiv a \pmod{m}$,
- (ii) se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$,
- (iii) se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Para verificar se dois números são congruentes módulo m , não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os seus restos. É suficiente aplicar o seguinte resultado:

Proposição 2.4. *Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \pmod{m}$ se, e somente se, $m \mid b - a$.*

Demonstração. Sejam $a, b, m \in \mathbb{Z}$ com $m > 1$. Suponha inicialmente que $a \equiv b \pmod{m}$. Isso significa que a e b possuem o mesmo resto na divisão por m , ou seja, existem inteiros q, q' e um número r com $0 \leq r < m$ tais que $a = mq + r$ e $b = mq' + r$. Subtraindo as duas expressões, segue que $b - a = m(q' - q)$. Como $q' - q$ é um número inteiro, concluímos que $m \mid b - a$.

Reciprocamente, suponha que $m \mid b - a$, ou seja, existe um inteiro k tal que $b - a = mk$, isto é,

$$b = a + mk. \quad (2.1)$$

Agora, dividindo a por m temos que existem inteiros q e r tais que

$$a = mq + r, 0 \leq r < m.$$

Substituindo na Equação 2.1, temos:

$$b = (mq + r) + mk = m(q + k) + r. \quad (2.2)$$

Como $q + k$ é inteiro, a expressão obtida na Equação 2.2 é precisamente a divisão euclidiana de b por m , com o mesmo resto r da divisão de a . Portanto, $a \equiv b \pmod{m}$, o que conclui a demonstração. $\square$

Todo número inteiro a é congruente módulo m ao seu resto pela divisão euclidiana por m . Para achar o resto da divisão de um número a por m , basta achar o número natural r dentre os números $0, \dots, m - 1$ que seja congruente a a módulo m .

Definição 2.5. Um *sistema completo de resíduos módulo m* é todo conjunto de números inteiros cujos restos pela divisão por m são os números $0, 1, \dots, m - 1$, sem repetições e numa ordem qualquer.

De acordo com a Definição 2.5, um sistema completo de resíduos módulo m possui m elementos. É claro que, se $a_1, \dots, a_m$ são m números inteiros, dois a dois não congruentes módulo m , então eles formam um sistema completo de resíduos módulo m . De fato, os restos da divisão dos a_i por m são dois a dois distintos, o que implica que são os números $0, 1, \dots, m - 1$ em alguma ordem.

Em particular, um conjunto formado por m inteiros consecutivos é um sistema completo de resíduos módulo m .

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

- i. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.*
- ii. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.*

Demonstração. Suponhamos que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Logo, temos que $m \mid b - a$ e $m \mid d - c$.

i) Note que $m \mid (b - a) + (d - c)$ e, portanto, $m \mid (b + d) - (a + c)$.

ii) Como $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, segue que existem $k_1, k_2 \in \mathbb{Z}$ tal que $b - a = mk_1$ e $d - c = mk_2$. Temos que $bd - ac = d(b - a) + a(d - c) = dm k_1 + am k_2$, para alguns $k_1, k_2 \in \mathbb{Z}$. Logo, $m \mid bd - ac$. $\square$

Corolário 2.7. *Para todos $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{m}$, então tem-se que $a^n \equiv b^n \pmod{m}$.*

Para a prova, basta usar indução sobre n e a Proposição 2.6 (ii).

Observação 2.8. Ao longo deste trabalho, adotaremos a notação usual da literatura, em que $\text{mdc}(a, b)$ denota o máximo divisor comum de a e b , enquanto $\text{mmc}(a, b)$ representa o mínimo múltiplo comum entre esses dois números inteiros.

Proposição 2.9. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que*

$$a + c \equiv b + c \pmod{m} \Leftrightarrow a \equiv b \pmod{m}.$$

Demonstração. Se $a \equiv b \pmod{m}$, segue-se imediatamente da Proposição 2.6(i) que $a + c \equiv b + c \pmod{m}$, pois $c \equiv c \pmod{m}$.

Reciprocamente, se $a + c \equiv b + c \pmod{m}$, então $m \mid b + c - (a + c)$, o que implica que $m \mid b - a$ e, consequentemente, $a \equiv b \pmod{m}$. $\square$

Não vale, em geral, o cancelamento para a multiplicação, como pode ser verificado no exemplo a seguir.

Exemplo 2.10. Como $4 \cdot 7 - 4 \cdot 3 = 16$ e $8 \mid 16$, temos que $4 \cdot 7 \equiv 4 \cdot 3 \pmod{8}$, e, no entanto, $7 \not\equiv 3 \pmod{8}$. Temos a seguir um resultado relacionado com o cancelamento multiplicativo.

Proposição 2.11. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Temos que*

$$ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{\text{mdc}(c, m)}}.$$

Demonstração. Mostraremos primeiramente que $\frac{m}{\text{mdc}(c, m)}$ e $\frac{c}{\text{mdc}(c, m)}$ são primos entre si.

Seja $d = \text{mdc}(c, m)$. Como d é o maior divisor comum de c e m , podemos escrever:

$$c = d \cdot c', \quad m = d \cdot m',$$

onde c' e m' são inteiros e primos entre si, ou seja,

$$\text{mdc}(c', m') = 1.$$

Dividindo as expressões acima por d , obtemos:

$$\frac{c}{d} = c', \quad \frac{m}{d} = m'.$$

Agora, queremos calcular

$$\text{mdc}\left(\frac{m}{d}, \frac{c}{d}\right) = \text{mdc}(m', c').$$

Como já foi estabelecido que $\text{mdc}(c', m') = 1$, segue que:

$$\text{mdc}\left(\frac{m}{\text{mdc}(c, m)}, \frac{c}{\text{mdc}(c, m)}\right) = 1.$$

Portanto, os números

$$\frac{m}{\text{mdc}(c, m)} \quad \text{e} \quad \frac{c}{\text{mdc}(c, m)}$$

são primos entre si.

Agora, temos que

$$\begin{aligned} ac \equiv bc \pmod{m} &\Leftrightarrow m \mid (b - a)c \Leftrightarrow \frac{m}{\text{mdc}(c, m)} \mid (b - a) \frac{c}{\text{mdc}(c, m)} \\ &\Leftrightarrow \frac{m}{\text{mdc}(c, m)} \mid b - a \Leftrightarrow a \equiv b \pmod{\frac{m}{\text{mdc}(c, m)}}. \end{aligned}$$

□

Corolário 2.12. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$ e $\text{mdc}(c, m) = 1$. Temos que*

$$ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{m}.$$

Proposição 2.13. *Sejam $a, k, m \in \mathbb{Z}$, com $m > 1$ e $\text{mdc}(k, m) = 1$. Se $a_1, \dots, a_m$ é um sistema completo de resíduos módulo m , então*

$$a + ka_1, \dots, a + ka_m$$

também é um sistema completo de resíduos módulo m .

Demonstração. Pela Proposição 2.9 e Corolário 2.12 para $i, j = 0, \dots, m - 1$, temos que

$$a + ka_i \equiv a + ka_j \pmod{m} \Leftrightarrow ka_i \equiv ka_j \pmod{m} \Leftrightarrow a_i \equiv a_j \pmod{m} \Leftrightarrow i = j.$$

Portanto $a + ka_1, \dots, a + ka_m$ são, dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m . □

Daremos, a seguir, algumas propriedades adicionais das congruências relacionadas com a multiplicação.

Proposição 2.14. *Sejam $a, b \in \mathbb{Z}$ e $m, n, m_1, \dots, m_r$ inteiros maiores do que 1. Temos que*

$$i. \text{ se } a \equiv b \pmod{m} \text{ e } n \mid m, \text{ então } a \equiv b \pmod{n};$$

ii. $a \equiv b \pmod{m_i}, \forall i = 1, \dots, r \Leftrightarrow a \equiv b \pmod{\text{mmc}(m_1, \dots, m_r)}$;

iii. se $a \equiv b \pmod{m}$, então $\text{mdc}(a, m) = \text{mdc}(b, m)$.

Demonstração. i) Se $a \equiv b \pmod{m}$, então $m \mid b - a$. Como $n \mid m$, segue-se que $n \mid b - a$. Logo, $a \equiv b \pmod{n}$.

ii) Se $a \equiv b \pmod{m_i}, i = 1, \dots, r$, então $m_i \mid b - a$, para todo i . Sendo $b - a$ um múltiplo de cada m_i , segue-se que $\text{mmc}(m_1, \dots, m_r) \mid b - a$, o que prova que $a \equiv b \pmod{\text{mmc}(m_1, \dots, m_r)}$.

A recíproca decorre do item (i).

iii) Se $a \equiv b \pmod{m}$, então $m \mid b - a$ e, portanto, $b = a + tm$ com $t \in \mathbb{Z}$. Logo, pelo Lema de Euclides, temos que

$$\text{mdc}(a, m) = \text{mdc}(a + tm, m) = \text{mdc}(b, m).$$

□

Corolário 2.15. Sejam a e b inteiros e sejam $m_1, m_2, \dots, m_k$ inteiros positivos tais que, para quaisquer $i, j \in \{1, \dots, k\}$ e $i \neq j$, $\text{mdc}(m_i, m_j) = 1$. Então,

$$a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$$

se, e somente se,

$$a \equiv b \pmod{(m_1 m_2 \dots m_k)}.$$

Demonstração. Por hipótese a e b são inteiros e $m_1, m_2, \dots, m_k$ são inteiros positivos que são primos entre si.

Primeiramente, suponha que $a \equiv b \pmod{m_i}$, para cada $i \in \{1, \dots, k\}$. Como o mmc de n números primos entre si é o produto destes n números, temos que $\text{mmc}(m_1, m_2, \dots, m_k) = m_1 m_2 \dots m_k$ já que os m_i são primos entre si. Assim, pela Proposição 2.14,

$$a \equiv b \pmod{(m_1 m_2 \dots m_k)}.$$

Por outro lado, suponha que $a \equiv b \pmod{(m_1 m_2 \dots m_k)}$. Então para cada m_i , usando propriedade de congruência, podemos ver que a é igual a b mais um múltiplo de m_i . Assim, $a \equiv b \pmod{m_i}$ para cada $m_i, i = 1, \dots, k$. □

Observação 2.16. Observe que a única restrição sobre a no Corolário 2.15 é que $a \in \mathbb{Z}$. Assim, podemos estender este resultado de modo que $x^n \equiv b \pmod{(m_1 m_2 \dots m_k)}$ se, e somente se, $x^n \equiv b \pmod{m_i}$ para cada m_i e $n \in \mathbb{N}$. Com isso temos uma ferramenta que nos permite transformar congruências em um sistema de equações. Vamos usar este resultado em nosso trabalho com reciprocidade no Capítulo 4.

Com a notação de congruências, o Pequeno Teorema de Fermat¹ enuncia-se como se segue:

Proposição 2.17. (Pequeno Teorema de Fermat - congruência) Se p é número primo e $a \in \mathbb{Z}$ com $\text{mdc}(a, p) = 1$, então

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

¹Pequeno Teorema de Fermat. Seja p um número primo e a um número inteiro que não é divisível por p . Então, o número $a^{p-1} - 1$ é divisível por p .

2.2 Critérios de divisibilidade via congruência

Nesta seção, apresentamos uma aplicação de congruência em critérios de divisibilidade.

Exemplo 2.18. Critérios de divisibilidade por 2, 5 e 10.

Primeiramente, observamos que a base decimal é múltipla de 2, 5 e 10, pois temos as seguintes congruências:

$$10 \equiv 0 \pmod{2}, \quad 10 \equiv 0 \pmod{5}, \quad 10 \equiv 0 \pmod{10}.$$

Isso significa que qualquer potência de 10 continua sendo múltipla de 2, 5 e 10, ou seja, para todo $i \geq 1$,

$$10^i \equiv 0 \pmod{2}, \quad 10^i \equiv 0 \pmod{5}, \quad 10^i \equiv 0 \pmod{10}. \quad (2.3)$$

Agora, consideremos um número natural n representado em sua forma decimal como

$$n = \sum_{i=0}^r n_i 10^i,$$

onde cada coeficiente n_i representa um dos dígitos do número e satisfaz $0 \leq n_i \leq 9$. Multiplicando as congruências da equação (2.3) por n_i segue que, para todo $i \geq 1$,

$$n_i 10^i \equiv 0 \pmod{2}, \quad n_i 10^i \equiv 0 \pmod{5}, \quad n_i 10^i \equiv 0 \pmod{10}.$$

Como cada termo $n_i 10^i$ para $i \geq 1$ é múltiplo de 2, 5 e 10, sua soma não afeta a congruência do número n . Assim, temos:

$$n \equiv n_0 \pmod{2}, \quad n \equiv n_0 \pmod{5}, \quad n \equiv n_0 \pmod{10}.$$

Portanto, um número n é divisível por 2, 5 ou 10 se, e somente se, o seu algarismo das unidades n_0 for divisível por 2, 5 ou 10, respectivamente.

Exemplo 2.19. Critérios de divisibilidade por 3 e 9.

Como $10 \equiv 1 \pmod{3}$ e $10 \equiv 1 \pmod{9}$, segue que $n_i 10^i \equiv n_i \pmod{3}$ e $n_i 10^i \equiv n_i \pmod{9}$. Isso mostra que, se n é representado na base 10 como $n_r n_{r-1} \dots n_0$, então

$$n \equiv (n_r + n_{r-1} + \dots + n_0) \pmod{3}$$

$$n \equiv (n_r + n_{r-1} + \dots + n_0) \pmod{9},$$

o que prova que n é divisível por 3 ou 9 se, e somente se, $n_r + n_{r-1} + \dots + n_0$ é divisível, respectivamente, por 3 ou por 9.

Exemplo 2.20. Critério de divisibilidade por 11.

Como $10 \equiv -1 \pmod{11}$, pelo Corolário 9.4, temos que $10^{2i} \equiv 1 \pmod{11}$ e $10^{2i+1} \equiv -1 \pmod{11}$.

Seja $n = n_T \cdots n_5 n_4 n_3 n_2 n_1 n_0$ um número escrito na base 10. Temos, então, que

$$\begin{aligned} n_0 &\equiv n_0 \pmod{11} \\ n_1 10 &\equiv -n_1 \pmod{11} \\ n_2 10^2 &\equiv n_2 \pmod{11} \\ n_3 10^3 &\equiv -n_3 \pmod{11}. \end{aligned}$$

Somando, membro a membro, as congruências acima, temos que

$$n = \sum_{i=0}^r n_i 10^i \equiv (n_0 - n_1 + n_2 - n_3 + \cdots) \pmod{11}.$$

Portanto, n é divisível por 11 se, e somente se, o número $n_0 - n_1 + n_2 - n_3 + \cdots$ é divisível por 11.

2.3 Congruências Lineares

Nesta seção examinaremos congruências lineares e estabelecemos quando soluções existirão. Em seguida, olhamos brevemente para as soluções de uma congruência quadrática módulo p , onde p é primo.

De acordo com a Definição 2.5, $\mathbb{Z}_m$ representa o anel dos inteiros módulo m , que é o conjunto dos restos da divisão de inteiros por m , ou seja,

$$\mathbb{Z}_m := \{0, 1, \dots, m-1\}.$$

Definição 2.21. Seja $n \in \mathbb{N}$ com $n \geq 2$. O grupo multiplicativo dos inteiros módulo n , denotado por $\mathbb{Z}_n^*$, é o conjunto das classes de equivalência de inteiros módulo n que são invertíveis com respeito à multiplicação módulo n . Ou seja,

$$\mathbb{Z}_n^* = \{ \bar{a} \in \mathbb{Z}_n \mid \text{mdc}(a, n) = 1 \}.$$

Equivalentemente, $\mathbb{Z}_n^*$ é o conjunto de todos os inteiros $a \in \{1, 2, \dots, n-1\}$ tais que existe $b \in \mathbb{Z}$ satisfazendo

$$ab \equiv 1 \pmod{n}.$$

Com a operação de multiplicação módulo n , o conjunto $\mathbb{Z}_n^*$ forma um grupo abeliano finito de ordem $\varphi(n)$, onde φ é a função totiente de Euler.

Teorema 2.22. Se $\text{mdc}(a, m) = d$, então $ax \equiv b \pmod{m}$ tem uma solução se, e somente se, $d \mid b$. Se uma solução existe, então existem exatamente d soluções distintas da congruência $ax \equiv b \pmod{m}$, essas soluções são incongruentes módulo m .

Demonstração. Seja $m \in \mathbb{N}$ e sejam $a, b \in \mathbb{Z}_m$. Suponha que s seja uma solução para $ax \equiv b \pmod{m}$. Então

$$\begin{aligned} as &\equiv b \pmod{m} \quad (s \text{ é uma solução}) \\ as - b &= km, \text{ para algum } k \in \mathbb{Z} \quad (\text{Proposição 2.4}) \\ b &= as - km. \end{aligned} \tag{2.4}$$

Mas, sabemos que d divide tanto a quanto m , já que $d = \text{mdc}(a, m)$, assim d divide o lado direito da Equação (2.4) e isso implica que d divide b também. Portanto, se temos uma solução para a congruência, então d divide b .

Agora queremos mostrar que, se $d \mid b$, então a congruência $ax \equiv b \pmod{m}$ possui solução. Como $d = \text{mdc}(a, m)$ existem $u, v \in \mathbb{Z}$ tais que

$$au + mv = d \text{ (pela identidade de Bézout)}$$

Suponha que $b = dk$ para algum $k \in \mathbb{Z}$ (isto é garantido pela hipótese $d \mid b$).

Multiplicando ambos os lados da identidade de Bézout por k , temos

$$k(au + mv) = kd$$

Substituindo $b = dk$, obtemos

$$a(ku) + m(kv) = b,$$

de onde segue que

$$a(ku) \equiv b \pmod{m}.$$

Portanto, $x_0 = ku$ é uma solução da congruência $ax \equiv b \pmod{m}$. Dessa forma, mostramos que uma solução existe.

Para a última parte, seja x_0 uma solução particular de $ax \equiv b \pmod{m}$, isto é, $ax_0 \equiv b \pmod{m}$. Como $\text{mdc}(a, m) = d$, podemos escrever $a = da'$, $m = dm'$ e $b = db'$, com $a', m', b' \in \mathbb{Z}$ e $\text{mdc}(a', m') = 1$. Substituindo esses valores na congruência original, obtemos:

$$da'x \equiv db' \pmod{dm'}.$$

Dividindo ambos os lados por d , obtemos a congruência:

$$a'x \equiv b' \pmod{m'},$$

a qual, por hipótese, tem $\text{mdc}(a', m') = 1$, ou seja, a' é inversível módulo m' . Assim, essa congruência admite uma única solução módulo m' , que denotamos por x'_0 . Como x_0 é uma solução da congruência original, sua redução módulo m' satisfaz $a'x \equiv b' \pmod{m'}$, de modo que $x'_0 \equiv x_0 \pmod{m'}$.

Para voltar à congruência original, observamos que toda solução x de $ax \equiv b \pmod{m}$ pode ser escrita na forma

$$x = x'_0 + m't,$$

onde t é um número inteiro. No entanto, cada uma dessas soluções, vista como elemento de $\mathbb{Z}_m$, repete-se se incrementarmos t em múltiplos de d , pois $m'd = m$. Portanto, escolhendo t para variar de 0 até $d - 1$, obtemos exatamente d soluções incongruentes entre si módulo m . Já valores de t fora desse intervalo conduzem a soluções que são congruentes a alguma das anteriores. Assim, concluímos que, se existe ao menos uma solução, então o total de soluções de $ax \equiv b \pmod{m}$ é exatamente $d = \text{mdc}(a, m)$. $\square$

Exemplo 2.23. Seja $a = 60$, $b = 45$ e $m = 90$. Então $\text{mdc}(60, 90) = 30$.

Queremos encontrar soluções para $60x \equiv 45 \pmod{90}$, se existirem. Pelo Teorema 2.22, haverá exatamente 30 soluções se, e somente se, $30 \mid 45$. Como 30 claramente não divide 45, a congruência não tem solução.

Teorema 2.24. Se p um número primo então $x^2 \equiv 1 \pmod{p}$ tem exatamente duas soluções, $x = 1$ e $x = p - 1$.

Demonstração. Note que

$$1^2 = 1 \equiv 1 \pmod{p}$$

e

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

Logo, tanto $x = 1$ quanto $x = -1$ satisfazem a congruência. Em seguida, observe que $p - 1 \equiv -1 \pmod{p}$, pois $p - 1 - (-1) = p$, que é múltiplo de p . Dessa forma, dizer que -1 é solução equivale a dizer que $p - 1$ é solução, concluindo, portanto, que $x = p - 1$ também satisfaz a congruência. Estamos trabalhando no corpo $\mathbb{Z}_p$ e em um corpo,² um polinômio de grau n tem no máximo n raízes distintas, ou seja, possui no máximo n soluções. Como exibimos duas soluções, para $f(x) = x^2 - 1 \in \mathbb{F}_p$, segue que para todo x^2 haverá apenas 2 soluções. $\square$

Lema 2.25. Se $d \mid (p - 1)$ e $p \in \mathbb{Z}$ é primo, então $x^d \equiv 1 \pmod{p}$ tem exatamente d soluções.

Demonstração. Por hipótese p é primo e suponha $d \mid (p - 1)$, para algum $d \in \mathbb{Z}$. Pelo Pequeno Teorema de Fermat, sabemos que se $\text{mdc}(a, p) = 1$, então $a^{p-1} \equiv 1 \pmod{p}$. Portanto, para cada $a \in \{1, \dots, p - 1\}$, $x = a$ é uma solução para $x^{p-1} \equiv 1 \pmod{p}$.

A fatoração de $x^{p-1} - 1$ resulta em

$$\begin{aligned} x^{p-1} - 1 &\equiv (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \dots + 1) \pmod{p} \\ &\equiv (x^d - 1) \cdot g(x) \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned} \quad (x^d \equiv 1 \pmod{p})$$

²Em matemática, um corpo é uma estrutura algébrica que consiste em um conjunto equipado com duas operações (adição e multiplicação) que satisfazem certas propriedades.

onde $g(x)$ é de grau $p - 1 - d$ e assim $g(x) = 0$ tem no máximo $p - 1 - d$ soluções. Como $x^{p-1} - 1 \equiv 0 \pmod{p}$ tem $p - 1$ soluções, segue-se que $x^d - 1 \equiv 0 \pmod{p}$ tem pelo menos d soluções. Mas se considerarmos $x^d - 1 \equiv 0 \pmod{p}$ isoladamente, vemos que ele tem no máximo d soluções. Para que ambos os resultados sejam verdadeiros, deve ser o caso de que ele tem exatamente d soluções. $\square$

Exemplo 2.26. Seja $p = 17$. Suponha $d = 4$ e considere $x^4 \equiv 1 \pmod{17}$. Claramente $x = 1$ é uma solução e $x = 16$ também é uma solução. Após alguns cálculos encontramos que $x = 4$ e $x = 13$ também são soluções, e verificamos que os outros doze elementos em $\{1, 2, \dots, 16\}$ não satisfazem a congruência, o que está de acordo com o Lema 2.25.

Teorema 2.27. (Teorema de Wilson) Um número p é primo se, e somente se,

$$(p - 1)! \equiv -1 \pmod{p}.$$

Demonstração. $(\Rightarrow)$ Suponha primeiro que $p = 2$. Então $(2 - 1)! = 1 \equiv -1 \pmod{2}$. Agora, suponha que $p \neq 2$ (portanto ímpar). Temos:

$$(p - 1)! = (p - 1) \cdot (p - 2) \dots 2 \cdot 1$$

Coloque $p - 1$ de lado por um momento e considere o resto do produto.

A identidade de Bézout afirma que, para quaisquer inteiros a e p , existem inteiros x e y tais que:

$$ax + py = \text{mdc}(a, p).$$

Quando p é primo e a pertence ao conjunto $\{2, \dots, p - 2\}$, sabemos que $\text{mdc}(a, p) = 1$. Assim, a equação de Bézout assume a forma: $ax + py = 1$. Tomando essa equação módulo p , obtemos:

$$ax \equiv 1 \pmod{p},$$

ou seja, o número x satisfaz a condição de ser o inverso multiplicativo de a módulo p , isto é, $x = a^{-1}$.

Como estamos trabalhando num corpo, esse resultado garante que para cada $a \in \{2, \dots, p - 2\}$, existe um único a^{-1} tal que $a \cdot a^{-1} \equiv 1 \pmod{p}$. Como o conjunto $\{2, \dots, p - 2\}$ tem um número par de elementos e os inversos aparecem em pares distintos, os produtos desses elementos se cancelam. Assim,

$$\begin{aligned} (p - 1)! &= (p - 1) \cdot (p - 2) \dots 3 \cdot 2 \cdot 1 \\ &\equiv (p - 1) \pmod{p} \\ &\equiv -1 \pmod{p}. \end{aligned}$$

$(\Leftarrow)$ Suponha que $p > 1$ não seja primo. Devemos considerar dois casos.

Caso 1: Seja $p = ab$ para $a, b \in \mathbb{Z}, 1 < a, b < p$. Sem perda de generalidade, assuma $b > a$. Então

$$\begin{aligned}(p-1)! &= (p-1)(p-2) \dots b \dots a \dots 2 \cdot 1 \\ &= abk, \text{ para } k = (p-1)(p-2) \dots 1 \dots 1 \dots 2 \cdot 1 \\ &\equiv 0 \pmod{p},\end{aligned}$$

o que contradiz a hipótese.

Caso 2: Seja $p = a^2$, então $a < p$. Se $p = 4$, então $3! = 6 \not\equiv -1 \pmod{4}$. Se $p \neq 4$, temos $(p-1)! = 2a^2k \equiv 0 \pmod{p}$, uma vez que a e $2a$ são ambos menores que $p-1$. Assim, por contraposição, se p não é primo, então $(p-1)! \not\equiv 1 \pmod{p}$. $\square$

Exemplo 2.28. Seja $p = 5$. Então temos $(5-1)! = 24 \equiv -1 \pmod{5}$. Em seguida, seja $p = 6$. Então $(6-1)! = 120 \equiv 0 \pmod{6}$ e assim, 6 não é primo.

Lema 2.29. Se n é um número inteiro ímpar, então

$$n^2 - 1 \equiv 0 \pmod{8}.$$

Demonstração. Lembre-se, da Definição 2.21, que $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. É claro que $k^2 \equiv 1 \pmod{8}$ para cada $k \in \mathbb{Z}_8^*$. Além disso, todo número ímpar n é congruente a um dos quatro elementos de $\mathbb{Z}_8^*$ módulo 8. Assim, $n^2 - 1 \equiv 0 \pmod{8}$ para cada n ímpar $\in \mathbb{Z}$. $\square$

Este é um resultado muito útil na teoria dos números e nós o usaremos quando olharmos para reciprocidade.

Definição 2.30. A função de Euler (também conhecida como função totiente de Euler), denotada por $\varphi(n)$, é o número de inteiros k , com $1 \leq k < n$, tais que $\text{mdc}(k, n) = 1$.

Definição 2.31. Seja m um inteiro positivo e seja $a \in \mathbb{Z}$ tal que $\text{mdc}(a, m) = 1$, ou seja, a é um elemento invertível no anel dos inteiros módulo m , $\mathbb{Z}_m$. Definimos a ordem multiplicativa de a módulo m , denotada por $\text{ord}_m(a)$, como o menor inteiro positivo t tal que

$$a^t \equiv 1 \pmod{m}.$$

Teorema 2.32. Seja $\text{mdc}(a, m) = 1$ e suponha que a tem ordem t módulo m . Então:

1. $a^n \equiv 1 \pmod{m}$ se, e somente se, $t \mid n$.
2. $t \mid \varphi(m)$.

Demonstração. Por hipótese temos $\text{mdc}(a, m) = 1$ e $a^t \equiv 1 \pmod{m}$.

1. ($\Rightarrow$) Suponha $a^n \equiv 1 \pmod{m}$. Pelo algoritmo da divisão, $n = qt + r$, onde $0 \leq r < t$. Assim,

$$\begin{aligned}a^n &\equiv 1 \pmod{m} \\ a^{qt+r} &\equiv 1 \pmod{m} \\ a^{qt} \cdot a^r &\equiv 1 \pmod{m} \\ (a^t)^q \cdot a^r &\equiv 1 \pmod{m} \\ a^r &\equiv 1 \pmod{m} \text{ (pois } a^t \equiv 1 \pmod{m}).\end{aligned}$$

Mas como $0 \leq r < t$, só teremos $a^r \equiv 1 \pmod{m}$ se $r = 0$. Portanto, $a^n \equiv 1 \pmod{m}$ somente se $t \mid n$.

($\Leftarrow$) Suponha agora que $t \mid n$. Então $n = tk$, para algum $k \in \mathbb{Z}$. Então

$$\begin{aligned} a^t &\equiv 1 \pmod{m} \\ (a^t)^k &\equiv 1^k \pmod{m} \\ a^{tk} &\equiv 1 \pmod{m} \\ a^n &\equiv 1 \pmod{m}, \end{aligned}$$

como desejado.

2. Pela Definição 2.21 a ordem de $\mathbb{Z}_m^*$ é $\varphi(m)$. O Teorema de Lagrange afirma que a ordem de um elemento divide a ordem do grupo, e como $a \in \mathbb{Z}_m^*$ tem ordem t , segue que $t \mid \varphi(m)$. $\square$

Teorema 2.33. *Seja t a ordem de $a \in \mathbb{Z}_m^*$. Então*

1. $a^r \equiv a^s \pmod{n}$ se, e somente se, $r \equiv s \pmod{t}$.
2. a^k tem ordem t se, e somente se, $\text{mdc}(k, t) = 1$.

Demonstração. Assuma que $a \in \mathbb{Z}_m^*$ tem ordem t módulo n .

1. ($\Rightarrow$) Como a é um elemento do grupo de unidades, tem um inverso multiplicativo módulo n . Suponha que $a^r \equiv a^s \pmod{n}$, e sem perda de generalidade, assumamos que $r \geq s$. Então

$$\begin{aligned} a^r &\equiv a^s \pmod{n} \\ a^{r-s} &\equiv 1 \pmod{n}. \end{aligned}$$

Como a tem ordem t , o que significa que t é o menor inteiro positivo tal que $a^t \equiv 1 \pmod{n}$. Assim se $t \mid r - s$, então $(r - s) = kt$ para algum $k \in \mathbb{Z}$, e $(r - s) \equiv 0 \pmod{t}$. Segue-se que $r \equiv s \pmod{t}$, por definição de congruência.

($\Leftarrow$) Suponha agora que $r \equiv s \pmod{t}$. Então $r = s + kt$ para algum $k \in \mathbb{Z}$, então

$$a^r \equiv a^{s+kt} \equiv a^s a^{kt} \equiv a^s (a^t)^k \equiv a^s \pmod{n}.$$

2. ($\Rightarrow$) Suponha que a e a^k ambos têm ordem t módulo m . Assuma que $\text{mdc}(k, t) = d$, para algum $d \in \mathbb{Z}^+$. Então $1 \equiv a^t \equiv (a^t)^{k/d} \equiv (a^k)^{t/d} \pmod{m}$. Mas a^k tem ordem t , portanto pelo Teorema 2.32, t/d é um múltiplo de t . Assim, para algum $l \in \mathbb{Z}$, temos

$$\begin{aligned} \frac{t}{d} &= tl \\ 1 &= dl \end{aligned}$$

Mas $d \in \mathbb{Z}^+$ e $l \in \mathbb{Z}$, então $d = 1$. Assim $\text{mdc}(k, t) = 1$.

($\Leftarrow$) Suponha que $\text{mdc}(k, t) = 1$, para algum $k \in \mathbb{N}$ e que a^k tenha ordem s módulo m . Então, como a tem ordem t , $1 \equiv (a^t)^k \equiv (a^k)^t \pmod{m}$. No entanto, o Teorema 2.32 afirma que t é um múltiplo de s , uma vez que a^k tem ordem s . Portanto, $t = js$ para algum $j \in \mathbb{Z}$, e assim $s \mid t$.

Também vale que $(a^k)^s \equiv a^{ks} \equiv 1 \pmod{m}$, então pelo Teorema 2.32, ks é um múltiplo de t , uma vez que a tem ordem t . Assim, $t \mid ks$. Mas pela hipótese,

$$\text{mdc}(k, t) = 1, \text{ e então, } t \mid s.$$

Agora temos $s \mid t$ e $t \mid s$, o que claramente implica que $s = t$, uma vez que ambos s e t são números naturais. Assim, a^k tem ordem t módulo m como desejado.

Segue que $a^r \equiv a^s \pmod{n}$ se, e somente se, $r \equiv s \pmod{t}$ e a^k tem ordem t se, e somente se, $\text{mdc}(k, t) = 1$. $\square$

Definição 2.34. Dizemos que $a \in \mathbb{Z}_n^*$ é uma *raiz primitiva módulo n* se $\langle a \rangle$ gera todo o grupo $\mathbb{Z}_n^*$, isto é, se $\langle a \rangle = \mathbb{Z}_n^*$.

Definição 2.35. Seja $a \in \mathbb{Z}_n^*$. O *subgrupo cíclico gerado por a* , denotado por $\langle a \rangle$, é definido como o conjunto

$$\langle a \rangle = \{ a^k \pmod{n} \mid k \in \mathbb{Z} \}.$$

Como $\mathbb{Z}_n^*$ é um grupo finito, esse conjunto coincide com

$$\langle a \rangle = \{ a^k \pmod{n} \mid 0 \leq k < \text{ord}_n(a) \},$$

onde $\text{ord}_n(a)$ denota a *ordem de a módulo n* , isto é, o menor inteiro positivo r tal que $a^r \equiv 1 \pmod{n}$.

Corolário 2.36. Se $\langle g \rangle = \mathbb{Z}_p^*$ para um primo p , então $\langle g^k \rangle = \mathbb{Z}_p^*$ se, e somente se, $\text{mdc}(k, p-1) = 1$.

Demonstração. Assuma que g é uma raiz primitiva de um primo p . Então g tem ordem $\varphi(p) = p-1$. Assim, $g^{p-1} \equiv 1 \pmod{p}$. Pelo Teorema 2.33, g^k tem ordem $p-1$ módulo p se, e somente se, $\text{mdc}(k, p-1) = 1$. Para que o menor resíduo de g^k seja uma raiz primitiva de p , devemos ter $0 \leq g^k \pmod{p} < p$ e a ordem de g^k módulo p deve ser $\varphi(p)$. Ambas as condições são atendidas se $\text{mdc}(k, p-1) = 1$, caso em que o menor resíduo de g^k será uma raiz primitiva de p . $\square$

Definição 2.37. Sejam m, n inteiros positivos e a qualquer inteiro, tal que $\text{mdc}(a, m) = 1$. Então dizemos que a é um *resíduo de potência n -ésima módulo m* se $x^n \equiv a \pmod{m}$ tem uma solução.

Casos particulares dessa definição incluem os resíduos quadráticos ($n = 2$) e cúbicos ($n = 3$), que possuem aplicações como por exemplo, em criptografia, testes de primalidade, teoria dos grafos, dentre outros. Sendo que o caso $n = 2$ será tratado detalhadamente no Capítulo 3.

Teorema 2.38. Seja m um inteiro positivo que possui raízes primitivas e seja $\text{mdc}(a, m) = 1$, para algum $a \in \mathbb{Z}$. Então a é um resíduo de potência n -ésima módulo m se, e somente se, $a^{\varphi(m)/d} \equiv 1 \pmod{m}$, onde $d = \text{mdc}(n, \varphi(m))$.

Demonstração. Suponha que m é um inteiro positivo e $d = \text{mdc}(n, \varphi(m))$ para algum $n \in \mathbb{N}$. Seja g uma raiz primitiva de m e seja $a = g^j$ e $x = g^k$, para inteiros positivos j e k . Então

$$\begin{aligned} x^n &\equiv a \pmod{m} \\ \iff g^{nk} &\equiv g^j \pmod{m} \\ \iff nk &\equiv j \pmod{\varphi(m)} \end{aligned} \quad (\text{Teorema 2.33})$$

Como $d \mid n$ e $d \mid \varphi(m)$, o Teorema 2.22 nos diz que $nk \equiv j \pmod{\varphi(m)}$ tem uma solução se, e somente se, $d \mid j$. Além disso, se uma solução existe, há exatamente d delas. Suponha que $d \mid j$. Então

$$\begin{aligned} a^{\varphi(m)/d} &\equiv (g^j)^{\varphi(m)/d} \\ &\equiv (g^{\varphi(m)})^{j/d} \\ &\equiv 1 \pmod{m} \end{aligned} \quad (g \text{ é uma raiz primitiva de } m)$$

Portanto, se a é um resíduo de potência n -ésima, $a^{\varphi(m)/d} \equiv 1 \pmod{m}$.

Suponha agora que $a^{\varphi(m)/d} \equiv 1 \pmod{m}$. Então

$$\begin{aligned} (g^j)^{\varphi(m)/d} &\equiv (g^{\varphi(m)})^{j/d} \\ &\equiv 1 \pmod{m}. \end{aligned}$$

Isso implica que $j\varphi(m)/d$ é um múltiplo de $\varphi(m)$, pelo Teorema 2.32. Assim, $j/d \in \mathbb{Z}$, então $d \mid j$. $\square$

Na seção seguinte, apresentaremos alguns resultados que servirão para a demonstração do Teorema Chinês do Resto. Este teorema desempenhará um papel fundamental na nossa análise da Lei da Reciprocidade Quadrática.

2.4 Teorema Chinês dos Resto

O Teorema Chinês dos Restos (TCR) é um resultado importante da teoria dos números, usado para resolver sistemas de congruências com módulos primos entre si. Ele ajuda a simplificar cálculos em aritmética modular. Na Lei da Reciprocidade Quadrática, o TCR é útil para reduzir problemas envolvendo resíduos quadráticos, especialmente quando há números compostos. Ele permite dividir o problema em módulos mais simples, facilitando o uso da lei em cada primo.

Lema 2.39. *Se $a_1, a_2, \dots, a_k$ são todos relativamente primos com n , então $a_1 a_2 \dots a_k$ também é relativamente primo com n .*

Demonstração. Assuma que $a_1 a_2 \dots a_k$ e n não são primos entre si. Então existe algum primo p tal que $p \mid n$ e $p \mid a_1 a_2 \dots a_k$. Como p é primo, p deve dividir algum a_i , o que implica que $\text{mdc}(a_i, n) \neq 1$. $\square$

Lema 2.40. *Se a e b dividem n e $\text{mdc}(a, b) = 1$, então ab divide n .*

Demonstração. Assuma que $\text{mdc}(a, b) = 1$ para alguns $a, b \in \mathbb{Z}$. A Identidade de Bézout afirma que, $ar + bs = 1$, para algum $r, s \in \mathbb{Z}$, e isso implica que $arn + bsn = n$. Mas $a \mid n$ significa que $al = n$ para algum $l \in \mathbb{Z}$. Da mesma forma, como $b \mid n$, há algum $k \in \mathbb{Z}$ tal que $bk = n$. Assim,

$$\begin{aligned} arn + bsn &= n \\ arb_k + bsal &= n \\ ab(rk + sl) &= n. \end{aligned}$$

Como $rk + sl \in \mathbb{Z}$, segue que $ab \mid n$. □

Lema 2.41. *Suponha que cada um dos $a_1, a_2, \dots, a_k$ divide n e $\text{mdc}(a_i, a_j) = 1$ para $i \neq j$. Então $a_1 a_2 \dots a_k \mid n$.*

Demonstração. Assuma que cada um dos $a_1, a_2, \dots, a_k$ divide algum n e assumamos também que $\text{mdc}(a_i, a_j) = 1$ para $i \neq j$. Usamos indução sobre k , onde o caso $k = 2$, é tratado pelo Lema 2.40. Assuma que o resultado é válido para algum $k - 1$, e considere k . Seja $a = a_1 a_2 \dots a_{k-1}$ e $b = a_k$. Então $a \mid n$ pela hipótese da indução e $\text{mdc}(a, b) = 1$, então pelo Lema 2.40, $ab = a_1 a_2 \dots a_k$ divide n . □

Teorema 2.42. *(Teorema Chinês dos Restos) Suponha que $m = m_1 m_2 \dots m_k$ e $\text{mdc}(m_i, m_j) = 1$ para $i \neq j$. Sejam $b_1, b_2, \dots, b_k$ inteiros e considere o sistema de congruências:*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_k \pmod{m_k}. \end{aligned}$$

Este sistema sempre tem soluções, e quaisquer duas soluções diferem apenas por um múltiplo de m .

Demonstração. Seja $n_i = \frac{m}{m_i}$. Então n_i é um produto de inteiros que são todos relativamente primos com m_i , portanto pelo Lema 2.39, $\text{mdc}(m_i, n_i) = 1$. Existem $x_i, y_i \in \mathbb{Z}$ tais que $m_i x_i + n_i y_i = 1$. Seja $e_i = n_i y_i$. Então $m_i x_i + e_i = 1$, o que implica que $e_i = 1 - m_i x_i$. Logo, $e_i \equiv 1 \pmod{m_i}$ pela definição de congruência, e $e_i \equiv 0 \pmod{m_j}$, uma vez que $\text{mdc}(m_i, m_j) = 1$ para todo $j \neq i$.

Defina $x_0 = \sum_{i=1}^k b_i e_i$. Então, $x_0 \equiv b_i e_i \equiv b_i \pmod{m_i}$ para todo $i \in \{1, 2, \dots, k\}$, implicando que x_0 é solução do sistema.

Suponha que x_1 seja qualquer outra solução. Então $x_1 - x_0 \equiv 0 \pmod{m_i}$, para $i \in \{1, 2, \dots, k\}$, ou seja, cada um dos m_i divide $(x_1 - x_0)$. Pelo Lema 2.41, segue que $m \mid (x_1 - x_0)$, e portanto o sistema dado de congruências sempre tem soluções, e qualquer par de soluções difere por algum múltiplo de m . □

Após a introdução de vários conceitos e alguns resultados importantes, no capítulo seguinte daremos início aos estudos sobre os Resíduos Quadráticos, o qual é essencial para a demonstração da Lei da Reciprocidade Quadrática.

3 Resíduos Quadráticos e Congruências Quadráticas

Iniciamos nossa exploração sobre reciprocidade quadrática definindo resíduos quadráticos e estabelecendo resultados sobre a solução de congruências quadráticas. Definimos o Critério de Euler em relação a soluções e, em seguida, estabelecemos alguns resultados sobre a solução de congruências de n -ésima potência. Definimos o símbolo de Legendre e provamos suas propriedades.

O estudo dos resíduos quadráticos, do critério de Euler e do símbolo de Legendre é essencial para a compreensão e aplicação da Lei da Reciprocidade Quadrática, um dos teoremas mais profundos e importantes da teoria dos números. Os resíduos quadráticos permitem determinar quando um número inteiro é quadrado módulo um número primo, e o símbolo de Legendre fornece uma maneira eficiente de expressar essa relação. Já o critério de Euler tem uma relação direta com a Lei da Reciprocidade Quadrática, pois ambos estão conectados ao conceito de resíduos quadráticos. As principais referências usadas para o desenvolvimento deste capítulo foram [8, 13, 10, 11, 12, 14, 15, 16, 9].

3.1 Resíduos Quadráticos

Abordaremos a seguir, resíduos quadráticos, um caso particular de resíduos de potência n -ésima definido no Capítulo 2. Resíduos quadráticos têm grande relevância em teoria dos números devido às suas aplicações em criptografia, aritmética modular e problemas clássicos envolvendo congruências quadráticas.

Definição 3.1. Se $\text{mdc}(a, m) = 1$, a é chamado de resíduo quadrático módulo m se a congruência $x^2 \equiv a \pmod{m}$ tem uma solução. Caso contrário, a é chamado de não resíduo quadrático módulo m .

Para simplificar, algumas vezes neste capítulo resíduos quadráticos podem ser referidos apenas como resíduos, e não resíduos quadráticos podem ser referidos como não resíduos.

Exemplo 3.2. Considere a congruência $x^2 \equiv a \pmod{7}$.

$$1^2 \equiv 1 \pmod{7}$$

$$2^2 \equiv 4 \pmod{7}$$

$$3^2 \equiv 2 \pmod{7}$$

$$4^2 \equiv 2 \pmod{7}$$

$$5^2 \equiv 4 \pmod{7}$$

$$6^2 \equiv 1 \pmod{7}.$$

Temos que 1, 2 e 4 são resíduos módulo 7, pois $x^2 \equiv 1 \pmod{7}$, $x^2 \equiv 2 \pmod{7}$ e $x^2 \equiv 4 \pmod{7}$ têm soluções. Por outro lado, 3, 5 e 6 são não resíduos módulo 7, pois $x^2 \equiv 3 \pmod{7}$, $x^2 \equiv 5 \pmod{7}$ e $x^2 \equiv 6 \pmod{7}$ não têm soluções.

Observe que isso particiona $\mathbb{Z}_7^*$ em dois conjuntos iguais de resíduos e não resíduos. Além disso, cada um dos resíduos tem exatamente duas soluções.

Teorema 3.3. Suponha que p seja um primo ímpar. Se $p \nmid a$, então $x^2 \equiv a \pmod{p}$ tem exatamente duas soluções ou não tem solução.

Demonstração. Assuma que $p \nmid a$ para algum $a \in \mathbb{Z}$ e algum primo ímpar p . Suponha que r seja uma solução para $x^2 \equiv a \pmod{p}$. Então $p - r$ também é uma solução, já que

$$(p - r)^2 = p^2 - 2pr + r^2 \equiv r^2 \pmod{p}.$$

Além disso, afirmamos que as duas soluções são distintas. Suponha que este não seja o caso. Então $r \equiv p - r \pmod{p}$ e, consequentemente, $2r \equiv p \pmod{p}$, ou seja, $2r \equiv 0 \pmod{p}$. Mas p é ímpar, então $\text{mdc}(2, p) = 1$. Isso implica que $r \equiv 0 \pmod{p}$. No entanto, $p \nmid r$, então isso é impossível. Assim, se r é uma solução, $p - r$ é uma solução diferente.

Um polinômio não nulo de grau n sobre um corpo tem no máximo n raízes distintas no corpo. Uma vez que $\mathbb{Z}_p$ é um corpo quando p é primo, e como o polinômio $x^2 - a$ tem grau 2, ele pode ter no máximo duas soluções em $\mathbb{Z}_p$. Portanto, se $x^2 \equiv a \pmod{p}$ tem uma solução, tem exatamente duas delas, e elas são $x = r$ e $x = p - r$. $\square$

Lema 3.4. Se g é uma raiz primitiva de p , então $g^{(p-1)/2} \equiv -1 \pmod{p}$.

Demonstração. Seja p um número primo e seja g uma raiz primitiva módulo p . Isso significa que g é um gerador do grupo multiplicativo $\mathbb{Z}_p^*$, que possui exatamente $\varphi(p) = p - 1$ elementos. Assim, a ordem de g em $\mathbb{Z}_p^*$ é $p - 1$, ou seja,

$$g^{p-1} \equiv 1 \pmod{p}.$$

Elevando ambos os lados à potência $1/2$, obtemos:

$$\left(g^{(p-1)/2}\right)^2 \equiv 1 \pmod{p}.$$

Portanto, $g^{(p-1)/2}$ é uma raiz quadrada de 1 no corpo $\mathbb{Z}_p$. As únicas soluções da congruência $x^2 \equiv 1 \pmod{p}$ são $x \equiv 1 \pmod{p}$ ou $x \equiv -1 \pmod{p}$. Assim, concluímos que:

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

Agora, suponha por contradição que $g^{(p-1)/2} \equiv 1 \pmod{p}$. Isso implicaria que a ordem de g divide $(p-1)/2$. No entanto, como g é uma raiz primitiva módulo p , sua ordem é exatamente $p-1$, o que contradiz a hipótese de que a ordem divide $(p-1)/2$.

Portanto, a única possibilidade restante é:

$$g^{(p-1)/2} \equiv -1 \pmod{p},$$

como queríamos demonstrar. □

Exemplo 3.5. Para encontrar os geradores de $\mathbb{Z}_{19}^*$, que é o grupo multiplicativo dos inteiros módulo 19, precisamos identificar os elementos cuja ordem é igual a $\varphi(19) = 18$. A ordem de um elemento $g \in \mathbb{Z}_{19}^*$ é o menor inteiro k tal que:

$$g^k \equiv 1 \pmod{19}.$$

Se a ordem de g é 18, então g é uma raiz primitiva de 19, pois suas potências $g^1, g^2, \dots, g^{18}$ percorrem todos os elementos de $\mathbb{Z}_{19}^*$.

Após os cálculos, encontramos que as raízes primitivas de 19 são $\{2, 3, 10, 13, 14, 15\}$. Aplicando o Lema 3.4 ao número 2 obtemos:

$$2^{(19-1)/2} = 2^9 \equiv -1 \pmod{19}.$$

Cálculos semelhantes valem para cada uma das outras raízes primitivas também.

Note que a recíproca do Lema 3.4 não é verdadeira. Podemos ver facilmente que:

$$8^9 \equiv 8^{23} \equiv 29^3 \equiv -1 \pmod{19}.$$

No entanto,

$$\begin{aligned} 8^1 &\equiv 8 \pmod{19}, \\ 8^2 &\equiv 7 \pmod{19}, \\ 8^3 &\equiv 18 \pmod{19}, \\ 8^4 &\equiv 11 \pmod{19}, \\ 8^5 &\equiv 12 \pmod{19}, \\ 8^6 &\equiv 1 \pmod{19}, \end{aligned}$$

então 8 não é uma raiz primitiva de 19, pois ele não é um gerador de $\mathbb{Z}_{19}^*$.

Lema 3.6. *Seja p primo com raiz primitiva g e seja $a = g^k$. Então $x^2 \equiv a \pmod{p}$ tem uma solução se, e somente se, k é par.*

Demonstração. Assuma que $x^2 \equiv a \pmod{p}$ tem uma solução, digamos g^l , para algum l . Então $(g^l)^2 \equiv a \pmod{p}$, o que implica que $g^{2l} \equiv a \pmod{p}$. Assim $k = 2l$ e então k é par.

Por outro lado, suponha agora que k é par. Então

$$x^2 \equiv g^k \pmod{p} \Leftrightarrow x^2 \equiv (g^{k/2})^2 \pmod{p},$$

mas como k é par, $k/2$ é um inteiro. Assim, $x^2 \equiv g^k \pmod{p}$ tem uma solução, a saber, $g^{k/2}$. $\square$

Teorema 3.7. (Critério de Euler) Se p é um primo ímpar e $p \nmid a$, então

$$a^{(p-1)/2} \equiv \begin{cases} 1 \pmod{p}, & \text{se } x^2 \equiv a \pmod{p} \text{ tem uma solução} \\ -1 \pmod{p}, & \text{se } x^2 \equiv a \pmod{p} \text{ não tem solução.} \end{cases}$$

Demonstração. Seja p um primo ímpar com raiz primitiva g . Então $g \in \mathbb{Z}_p^*$ e a ordem de g módulo p é $\varphi(p)$, assim $g^{p-1} \equiv 1 \pmod{p}$.

Considere a congruência $x^2 \equiv a \pmod{p}$. Como $a \in \mathbb{Z}_p^*$, $a \equiv g^k \pmod{p}$, para algum $1 \leq k \leq p-1$. Se uma solução para a congruência existir, então k é par, pelo Lema 3.6. Assim,

$$\begin{aligned} a^{(p-1)/2} &\equiv (g^k)^{(p-1)/2} \pmod{p} \\ &\equiv (g^{p-1})^{k/2} \pmod{p} \\ &\equiv 1 \pmod{p}. \end{aligned} \quad \text{(Pequeno Teorema de Fermat)}$$

Portanto, $a^{(p-1)/2} \equiv 1 \pmod{p}$ se uma solução existir.

Agora, uma direção do Lema 3.6 diz que se há uma solução para $x^2 \equiv a \pmod{p}$, então k é par. Assim, a outra positiva diz que se k é ímpar, então não há solução. Suponha que k seja ímpar. Então, como $a \equiv g^k \pmod{p}$,

$$\begin{aligned} a^{(p-1)/2} &\equiv (g^k)^{(p-1)/2} \pmod{p} \\ &\equiv (g^{(p-1)/2})^k \pmod{p} \\ &\equiv (-1)^k \pmod{p} \\ &\equiv -1 \pmod{p}. \end{aligned} \quad \text{(Lema 3.4)}$$

Combinando esses resultados, temos $a^{(p-1)/2} \equiv 1 \pmod{p}$ se $x^2 \equiv a \pmod{p}$ tem uma solução, e $a^{(p-1)/2} \equiv -1 \pmod{p}$ se $x^2 \equiv a \pmod{p}$ não tem solução. $\square$

Exemplo 3.8. Pelo Exemplo 3.2, $x^2 \equiv 3 \pmod{7}$ não tem solução, e pelo Critério de Euler resulta em $3^{(7-1)/2} \equiv -1 \pmod{7}$. Há duas soluções para $x^2 \equiv 4 \pmod{7}$, e o Critério de Euler resulta em $4^{(7-1)/2} \equiv 1 \pmod{7}$.

Se examinarmos $x^2 \equiv 1 \pmod{7}$, veremos que também há duas soluções e pelo Critério de Euler resulta em $1^{(7-1)/2} \equiv 1 \pmod{7}$. De fato, como $1^k \equiv 1$ para qualquer $k \in \mathbb{N}$, 1 sempre será um resíduo quadrático para qualquer primo p . Isso decorre do fato de que $x^2 - 1 \equiv 0 \pmod{7}$ sempre tem exatamente duas soluções, já que $\mathbb{Z}_p$ é um corpo.

Corolário 3.9. *Há tantos resíduos quadráticos quanto não resíduos quadráticos módulo p .*

Demonstração. Suponha que $x^2 \equiv a \pmod{p}$ tenha uma solução para algum primo p . Então, pelo Critério de Euler, $a^{(p-1)/2} \equiv 1 \pmod{p}$. Claramente, $\frac{p-1}{2} \mid p-1$, então pelo Lema 2.25, sabemos que $a^{(p-1)/2} \equiv 1 \pmod{p}$ tem exatamente $\frac{p-1}{2}$ soluções. Assim, há exatamente $\frac{p-1}{2}$ valores de a para os quais o Critério de Euler nos diz que $x^2 \equiv a \pmod{p}$ tem uma solução, então há exatamente $\frac{p-1}{2}$ resíduos quadráticos. Mas há $p-1$ elementos em $\mathbb{Z}_p^*$, então há $p-1 - \left(\frac{p-1}{2}\right) = \frac{p-1}{2}$ não resíduos também. $\square$

Teorema 3.10. *Suponha que p seja um primo ímpar. Seja $a \in \mathbb{Z}$ e $n \in \mathbb{N}$ tal que $p \nmid a$ e $p \nmid n$. Se $x^n \equiv a \pmod{p}$ tem solução, então $x^n \equiv a \pmod{p^e}$ tem solução para todo $e \geq 1$. Além disso, para qualquer n dado, essas congruências têm o mesmo número de soluções.*

Exemplo 3.11. Considere a congruência $x^2 \equiv 2 \pmod{5}$.

x	1	2	3	4
$x^2 \pmod{5}$	1	4	4	1

Note que nenhum dos resíduos é equivalente a 2 módulo 5, portanto, essa congruência não tem solução.

Considere $x^2 \equiv 4 \pmod{5}$. Podemos verificar que $x = 2$ e $x = 3$ são soluções. Portanto, a congruência possui solução para $e = 1$.

Se $e = 2$, a congruência torna-se $x^2 \equiv 2 \pmod{25}$.

x	1	2	3	4	5	6	7	8	9	10	11	12
$x^2 \pmod{25}$	1	4	9	16	0	11	24	14	6	0	21	19
x	13	14	15	16	17	18	19	20	21	22	23	24
$x^2 \pmod{25}$	19	21	0	6	14	24	11	0	16	9	4	1

Novamente não possuímos nenhum resíduo equivalente a 2 módulo 25, então tal congruência não possui solução. No entanto, se $e = 2$, podemos ver que $x = 2$ e $x = 23$ são soluções para $x^2 \equiv 4 \pmod{25}$.

Lembre-se que no Teorema 2.38 vimos que se m é um inteiro positivo que possui raízes primitivas e a e m são relativamente primos, então a é um resíduo de potência n -ésima módulo m se, e somente se, $a^{\varphi(m)/d} \equiv 1 \pmod{m}$, onde $d = \text{mdc}(n, \varphi(m))$. Lembre-se também que ter raízes primitivas em m significa que há algum elemento $g \in \mathbb{Z}_m^*$, tal que $\langle g \rangle \in \mathbb{Z}_m^*$.

Considere a congruência $x^n \equiv a \pmod{m}$, onde $m \in \mathbb{Z}^*$. Podemos expressar m por sua decomposição em potências de primos, de modo que $m = 2^e p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, onde cada p_i é distinto, e cada e_i são números naturais. Então, pelo Corolário 2.15, $x^n \equiv a \pmod{2^e p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}}$ pode ser escrito como um sistema de congruências:

$$\begin{aligned} x^n &\equiv a \pmod{2^e} \\ x^n &\equiv a \pmod{p_1^{e_1}} \\ &\vdots \\ x^n &\equiv a \pmod{p_k^{e_k}}, \end{aligned}$$

assim, $x^n \equiv a \pmod{2^e p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}}$ tem solução se, e somente se, o sistema de congruências tem solução.

Proposição 3.12. *Suponha que a seja ímpar e $e \geq 3$. Considere a congruência $x^n \equiv a \pmod{2^e}$.*

1. *Se n é ímpar, sempre existe uma solução única.*
2. *Se n é par, uma solução existe se, e somente se, $a \equiv 1 \pmod{4}$ e $a^{(2^{e-2})/d} \equiv 1 \pmod{2^e}$, onde $d = \text{mdc}(n, 2^{e-2})$. Quando uma solução existe, há exatamente 2^d delas.*

Uma ideia da prova desta proposição pode ser encontrada em [[17], Prop. 4.2.4, p. 62].

Teorema 3.13. *Seja 2^l a maior potência de 2 que divide n . Suponha que a seja ímpar e que $x^n \equiv a \pmod{2^{2l+1}}$ tenha solução. Então $x^n \equiv a \pmod{2^e}$ tem solução para todo $e \geq 2l+1$. Além disso, todas essas congruências têm o mesmo número de soluções.*

Demonstração. Assuma que $x^n \equiv a \pmod{2^m}$ tem uma solução para algum $m \geq 2l+1$. Seja x_0 essa solução e tome $x_1 = x_0 + 2^{m-l}b$. Então, considerando a expansão binomial, temos

$$\begin{aligned} x_1^n &= (x_0 + 2^{m-l}b)^n \\ &= \binom{n}{0}x_0^n + \binom{n}{1}x_0^{n-1}2^{m-l}b + \binom{n}{2}x_0^{n-2}(2^{m-l}b)^2 + \dots + \binom{n}{n}(2^{m-l}b)^n \\ &= x_0^n + nx_0^{n-1}2^{m-l}b + \binom{n}{2}x_0^{n-2}2^{2m-2l}b^2 + \dots + \binom{n}{n}2^{mn-ln}b^n. \end{aligned}$$

Agora iremos examinar o outro lado do módulo 2^{m+1} . Veja que se $m = 2l+1$, então

$$\begin{aligned} 2m - 2l &= 2(2l+1) - 2l \\ &= 2l + 2 \\ &= m + 1. \end{aligned}$$

Então $\binom{n}{2}x_0^{n-2}2^{2m-2l}b^2 \equiv 0 \pmod{2^{m+1}}$ sem considerar m , pois $m \geq 2l+1$. Os termos que seguem este são equivalentes a 0 módulo 2^{m+1} , pois seus expoentes de base 2 são ainda maiores, assim $x_1^n \equiv x_0^n + nx_0^{n-1}2^{m-l}b \pmod{2^{m+1}}$.

Queremos que essa congruência esteja na forma $x_1^n \equiv a \pmod{2^{m+1}}$. Para isso, lembre-se que $x_0^n \equiv a \pmod{2^m}$ implica que existe $k \in \mathbb{Z}$ tal que $a - x_0^n = 2^m k$, então $k = \frac{a-x_0^n}{2^m} \in \mathbb{Z}$. Precisamos encontrar $b \in \mathbb{Z}$ tal que $nx_0^{n-1}b \equiv \frac{a-x_0^n}{2^{m-l}} \pmod{2^{l+1}}$. Esta é uma congruência linear em b , então podemos aplicar o Teorema 2.22. Se $\text{mdc}(nx_0^{n-1}, 2^{l+1}) = d = 1$, uma solução única existe.

Como $2^{l+1} \nmid nx_0^{n-1}$ por hipótese, $d = 1$. Assim, existe exatamente um b que satisfaz a congruência.

Como $nx_0^{n-1}b \equiv \frac{a-x_0^n}{2^{m-l}} \pmod{2^{l+1}}$, existe algum $j \in \mathbb{Z}$ tal que $s^{l+1}j = 2^{m-l}nx_0^{n-1}b - \frac{a-x_0^n}{2^{m-l}}$, pela definição de congruência. Eliminando as frações e simplificando essa equação, temos

$2^{m+1}j + a = 2^{m-l}nx_0^{n-1}b + x_0^n$. Mas isso implica que $2^{m-l}nx_0^{n-1}b + x_0^n \equiv a \pmod{2^{m+1}}$. Com este valor de b , temos $x_1^n \equiv x_0^n + 2^{m-l}nx_0^{n-1}b \equiv a \pmod{2^{m+1}}$, que é exatamente o resultado que precisávamos.

Finalmente, precisamos mostrar que, para qualquer n , as congruências têm o mesmo número de soluções. Vimos no Teorema 2.38 que, se uma solução existe, então há exatamente $\text{mdc}(n, \varphi(p^e))$ soluções. Assim, precisamos mostrar que $\text{mdc}(n, \varphi(p)) = \text{mdc}(n, \varphi(p^e))$.

Seja $d = \text{mdc}(n, \varphi(p)) = \text{mdc}(n, p-1)$. Então $d \mid n$ e $d \mid p-1$. Precisamos mostrar que $d = \text{mdc}(n, \varphi(p^e))$. Sabemos que $\varphi(p^e) = p^{e-1}(p-1)$. Portanto, precisamos de $d = \text{mdc}(n, p^{e-1}(p-1))$. Como p é primo, $d \nmid p^{e-1}$, mas $d \mid n$ e $d \mid p-1$, segue que $\text{mdc}(n, p^{e-1}(p-1)) = d$, como desejado. Assim, ambas as congruências têm exatamente o mesmo número de soluções, independentemente do valor de n . $\square$

Exemplo 3.14. Seja $n = 6$. Então, como $2^1 \mid 6$, temos $l = 1$. Suponha que $x^6 \equiv a \pmod{2^3}$ tem solução. Note que como

$$1^6 \equiv 1 \pmod{8}$$

$$2^6 \equiv 0 \pmod{8}$$

$$3^6 \equiv 1 \pmod{8}$$

$$4^6 \equiv 0 \pmod{8}$$

$$5^6 \equiv 1 \pmod{8}$$

$$6^6 \equiv 0 \pmod{8}$$

$$7^6 \equiv 1 \pmod{8}$$

e o Teorema 3.13 afirma que a precisa ser ímpar, segue que se $a \equiv 1$, temos as possíveis soluções $x \equiv 1, x \equiv 3, x \equiv 5$ ou $x \equiv 7$. Além disso, se $x^6 \equiv a \pmod{2^3}$ tiver solução, então $x^6 \equiv a \pmod{2^e}$ também tem solução, para todo $e \geq 3$.

Se examinarmos a congruência para $e = 4$, temos $x^6 \equiv 1 \pmod{16}$. Claramente, $x = 1$ também é uma solução, assim essa congruência tem solução. De fato, 1 será uma solução para qualquer escolha positiva de e , portanto o resultado se mantém.

Teorema 3.15. Seja $m = 2^e p_1^{e_1} \dots p_k^{e_k}$ a decomposição prima de m , e suponha que $\text{mdc}(a, m) = 1$. Então $x^2 \equiv a \pmod{m}$ tem solução se, e somente se, as seguintes condições forem satisfeitas:

1. Se $e = 2$, então $a \equiv 1 \pmod{4}$.

Se $e \geq 3$, então $a \equiv 1 \pmod{8}$.

2. Para cada $1 \leq i \leq k$, temos $a^{(p_i-1)/2} \equiv 1 \pmod{p_i}$.

Demonstração. Começamos observando que se $e = 0$, nenhuma condição adicional é necessária, e se $e = 1$, então a deve ser ímpar — o que já é garantido pois $\text{mdc}(a, m) = 1$. Seja $m = 2^e p_1^{e_1} \dots p_k^{e_k} \in \mathbb{Z}$ e suponha que $\text{mdc}(a, m) = 1$ para algum $a \in \mathbb{Z}$. Considere a

congruência $x^2 \equiv a \pmod{(2^e p_1^{e_1} \cdots p_k^{e_k})}$. Pelo Corolário 2.15, $x^2 \equiv a \pmod{2^e p_1^{e_1} \cdots p_k^{e_k}}$ é equivalente ao sistema de congruências:

$$\begin{aligned} x^2 &\equiv a \pmod{2^e} \\ x^2 &\equiv a \pmod{p_1^{e_1}} \\ &\vdots \\ x^2 &\equiv a \pmod{p_k^{e_k}}. \end{aligned}$$

Considere $x^2 \equiv a \pmod{2^e}$. Se $e = 2$, então $x^2 \equiv a \pmod{4}$, e

$$1^2 \equiv 1 \pmod{4}$$

$$2^2 \equiv 0 \pmod{4}$$

$$3^2 \equiv 1 \pmod{4}.$$

Observe que, como $\text{mdc}(a, m) = 1$, a deve ser necessariamente ímpar, já que m é par. Então $a \equiv 1 \pmod{4}$ implica que $x^2 \equiv a \pmod{2^e}$ tem uma solução. Para satisfazer o requisito de se e somente se do teorema, suponha que $x^2 \equiv a \pmod{4}$ tenha solução e $\text{mdc}(a, 4) = 1$. Então, pelas considerações anteriores, a é necessariamente congruente a 1 módulo 4. Com isso, segue que se $e = 2$, então $x^2 \equiv a \pmod{4}$ tem solução se, e somente se, $a \equiv 1 \pmod{4}$.

Agora suponha $e = 3$. Então para $x^2 \equiv a \pmod{8}$, temos

$$1^2 \equiv 1 \pmod{8}$$

$$2^2 \equiv 4 \pmod{8}$$

$$3^2 \equiv 1 \pmod{8}$$

$$4^2 \equiv 0 \pmod{8}$$

$$5^2 \equiv 1 \pmod{8}$$

$$6^2 \equiv 4 \pmod{8}$$

$$7^2 \equiv 1 \pmod{8}.$$

Novamente sabemos que a é ímpar, então $a \equiv 1 \pmod{8}$ implica que $x^2 \equiv a \pmod{8}$ tem uma solução. A solução é possível pelo Teorema 3.3, se $x^2 \equiv a \pmod{8}$ tiver solução, então $x^2 \equiv a \pmod{2^e}$ também tem solução para todo $e \geq 3$.

Agora considere $x^2 \equiv a \pmod{p_i^{e_i}}$. Como cada p_i é um primo ímpar, $\text{mdc}(2, p_i) = 1$. Pelo Teorema 3.10, se $x^2 \equiv a \pmod{p_i}$ tiver solução, então $x^2 \equiv a \pmod{p_i^{e_i}}$ também tem solução.

Suponha que $x^2 \equiv a \pmod{p_i^{e_i}}$ tenha uma solução, digamos r . Então $r^2 \equiv a \pmod{p_i^{e_i}}$, o que implica que $r^2 \equiv a + \alpha p_i^{e_i}$, e assim $r^2 = a + \beta p_i$, onde $\beta = \alpha p_i^{e_i-1}$. Mas isso implica que $r^2 \equiv a \pmod{p_i}$, então r também é uma solução para a congruência $x^2 \equiv a \pmod{p_i}$. Segue-se que $x^2 \equiv a \pmod{p_i^{e_i}}$ tem solução se, e somente se, $x^2 \equiv a \pmod{p_i}$ tem solução.

Agora estamos na condição de aplicar o Teorema 2.38 com $n = 2$, $m = p_i$ e $d = \text{mdc}(n, \varphi(m)) = \text{mdc}(2, p_i - 1) = 2$. O teorema indica que $x^2 \equiv a \pmod{p_i}$ tem solução se, e somente se, $a^{(p_i-1)/2} \equiv 1 \pmod{p_i}$. $\square$

Exemplo 3.16. Seja $m = 72$. Então a decomposição em números primos de 72 é $72 = 2^3 3^2$. Considere a congruência $x^2 \equiv a \pmod{72}$. Pelo Teorema 3.15, $e = 3$ e esta congruência tem uma solução se, e somente se, $a \equiv 1 \pmod{8}$.

Suponha $a = 35$. Como $35 \equiv 3 \pmod{8}$, $x^2 \equiv 35 \pmod{72}$ não tem solução.

Se $a = 41$ então $41 \equiv 1 \pmod{8}$, mas se considerarmos o segundo requisito (item 2) do Teorema 3.15, para $p = 3$, temos $41^{(3-1)/2} \equiv 41 \equiv 2 \pmod{3}$. Portanto, a condição 2 não é satisfeita, e não há solução para $x^2 \equiv 41 \pmod{72}$.

Seja $a = 49$. Então $49 \equiv 1 \pmod{8}$ e $49^{(3-1)/2} \equiv 49 \equiv 1 \pmod{3}$, então a congruência $x^2 \equiv 49 \pmod{72}$ tem uma solução pelo Teorema 3.15. A solução parece intuitiva, já que $x \equiv 7$ claramente satisfaz a congruência.

3.2 Símbolo de Legendre

O restante deste capítulo será dedicado à exploração de congruências da forma $x^2 \equiv a \pmod{p}$ e à determinação se elas têm ou não soluções. A. M. Legendre criou uma notação chamada *símbolo de Legendre*, que representa a frase “a congruência $x^2 \equiv a \pmod{p}$ tem uma solução” onde esta será um resíduo quadrático ou não.

Definição 3.17. Seja p um primo ímpar e $a \in \mathbb{Z}$. O símbolo de Legendre $\left(\frac{a}{p}\right)$ é definido por

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

Notação: O símbolo de Legendre pode ser escrito como (a/p) ou como $\left(\frac{a}{p}\right)$.

Observe que o caso especial de $\left(\frac{a}{2}\right)$ não é abordado nesta definição. Se examinarmos a congruência $x^2 \equiv a \pmod{2}$, nossas únicas escolhas são $a \equiv 0$ e $a = 1$. Se $a = 1$, então claramente $x = 1$ é uma solução. De fato, qualquer inteiro ímpar é uma solução quando estamos trabalhando com módulo 2.

Teorema 3.18. (*Propriedades do Símbolo de Legendre*)

1. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.
2. Se $p \nmid a$ e $p \nmid b$, então $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.
3. Se $a \equiv b \pmod{p}$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
4. Se $p \nmid a$, então $\left(\frac{a^2}{p}\right) = 1$.
5. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \pmod{4} \\ -1, & \text{se } p \equiv 3 \pmod{4}. \end{cases}$

Demonstração. Suponha que p seja um primo ímpar e considere a congruência $x^2 \equiv a \pmod{p}$.

1. A Propriedade 1 segue imediatamente do Critério de Euler (Teorema 3.7).
2. Suponha que $p \nmid a$ e $p \nmid b$. Então

$$\begin{aligned} \left(\frac{ab}{p}\right) &\equiv (ab)^{\frac{p-1}{2}} \pmod{p} && \text{(Propriedade 1 dos símbolos de Legendre)} \\ &\equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod{p} \\ &\equiv \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}. && \text{(Propriedade 1 dos símbolos de Legendre).} \end{aligned}$$

3. Suponha $a \equiv b \pmod{p}$. Então $x^2 \equiv a \pmod{p}$ e $x^2 \equiv b \pmod{p}$ são a mesma congruência, portanto, ou ambas têm soluções ou ambas não têm.

4. Suponha que $p \nmid a$. Então $x^2 \equiv a^2 \pmod{p}$ claramente tem uma solução, especificamente o menor resíduo de a módulo p . Assim, $\left(\frac{a^2}{p}\right) = 1$.

5. Suponha que $p \equiv 1 \pmod{4}$. Então $p = 4k + 1$ para algum $k \in \mathbb{Z}$. Considere $x^2 \equiv -1 \pmod{p}$. Pela Propriedade 1 do símbolo de Legendre, temos

$$\begin{aligned} (-1)^{\frac{p-1}{2}} &\equiv (-1)^{(4k+1-1)/2} \pmod{p} && (p = 4k + 1) \\ &\equiv (-1)^{2k} \pmod{p} \\ &\equiv 1 \pmod{p}. \end{aligned}$$

Suponha que $p \equiv 3 \pmod{4}$. Então $p = 4j + 3$, para algum $j \in \mathbb{Z}$. Considere $x^2 \equiv -1 \pmod{p}$. Pela Propriedade 1 do símbolo de Legendre, temos

$$(-1)^{\frac{p-1}{2}} \equiv (-1)^{(4j+3-1)/2} \pmod{p} \quad (p = 4j + 3) \quad (3.1)$$

$$\equiv (-1)^{2j+1} \pmod{p} \quad (3.2)$$

$$\equiv -1 \pmod{p}. \quad (3.3)$$

Portanto,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \pmod{4} \\ -1, & \text{se } p \equiv 3 \pmod{4}. \end{cases}$$

Segue assim que todas as cinco propriedades são válidas como desejado. $\square$

Observe que as propriedades do símbolo de Legendre indicam que o produto de dois resíduos quadráticos é novamente um resíduo. Se a e b são resíduos módulo p , então $\left(\frac{a}{p}\right) = 1$ e $\left(\frac{b}{p}\right) = 1$ e certamente multiplicar esses resultados também resulta em 1, então ab é também um resíduo. Por outro lado, se a é um resíduo e b é um não-resíduo, então $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = 1 \cdot (-1) = -1$, e ab é um não-resíduo. Portanto, o produto de um resíduo e um não-resíduo é um não-resíduo. Isso significa que o símbolo de Legendre pode ser interpretado como um caráter multiplicativo.

Exemplo 3.19. Considere o símbolo de Legendre $\left(\frac{87}{101}\right)$. Pela Propriedade 2 (Teorema 3.18), isso se torna:

$$\left(\frac{87}{101}\right) = \left(\frac{3}{101}\right) \left(\frac{29}{101}\right).$$

Agora, se aplicarmos a Propriedade 1 a cada um dos símbolos de Legendre no lado direito, temos:

$$\begin{aligned} \left(\frac{3}{101}\right) &\equiv 3^{\frac{101-1}{2}} \pmod{101} && \text{(Propriedade 1 do símbolo de Legendre)} \\ &\equiv 3^{50} \pmod{101} \\ &\equiv -1 \pmod{101} && \text{(Redução módulo 101)} \end{aligned}$$

e

$$\begin{aligned} \left(\frac{29}{101}\right) &\equiv 29^{\frac{101-1}{2}} \pmod{101} && \text{(Propriedade 1 do símbolo de Legendre)} \\ &\equiv 29^{50} \pmod{101} \\ &\equiv -1 \pmod{101}. && \text{(Redução módulo 101)} \end{aligned}$$

Assim,

$$\left(\frac{87}{101}\right) = (-1)(-1) = 1 \pmod{101},$$

então $x^2 \equiv 87 \pmod{101}$ tem uma solução pela definição do símbolo de Legendre.

Usando o software *Mathematica* para os cálculos, descobrimos que $x \equiv 17$ e $x \equiv 84$ são as duas soluções.

Exemplo 3.20. Considere a congruência $x^2 \equiv 3870 \pmod{431}$. Como $3870 \equiv 422 \pmod{431}$, pela Propriedade 3 do símbolo de Legendre, $\left(\frac{3870}{431}\right) = \left(\frac{422}{431}\right)$.

Assim, se avaliarmos ambos os símbolos, eles devem nos dar o mesmo resultado. Para o primeiro símbolo,

$$\begin{aligned} \left(\frac{3870}{431}\right) &= \left(\frac{430 \cdot 3^2}{431}\right) \\ &= \left(\frac{-1 \cdot 3^2}{431}\right) && (430 \equiv -1 \pmod{431}) \\ &= \left(\frac{-1}{431}\right) \left(\frac{3}{431}\right)^2 && \text{(Propriedade 2 dos símbolos de Legendre)} \\ &\equiv (-1)(1) \pmod{431} && \text{(Propriedades 3 e 5 dos símbolos de Legendre)} \\ &\equiv -1 \pmod{431}. \end{aligned}$$

Para o segundo,

$$\begin{aligned}
 \left(\frac{422}{431}\right) &= \left(\frac{2}{431}\right) \left(\frac{211}{431}\right) && \text{(Propriedade 2 dos símbolos de Legendre)} \\
 &\equiv 2^{\frac{431-1}{2}} \cdot 211^{\frac{431-1}{2}} \pmod{431} && \text{(Propriedade 1 dos símbolos de Legendre)} \\
 &\equiv 2^{215} \cdot 211^{215} \pmod{431} \\
 &\equiv (1)(-1) \pmod{431} && \text{(Reduzido modulo 431)} \\
 &\equiv -1 \pmod{431},
 \end{aligned}$$

confirmando a Propriedade 3. Pela Definição 3.17 segue que ambos não são resíduos quadráticos módulo 431.

Lema 3.21. (Lema de Gauss) *Seja p um primo ímpar e $p \nmid a$. Considere os inteiros $a, 2a, 3a, \dots, \frac{p-1}{2}a$ e seus menores resíduos positivos módulo p . Se n conta o número desses resíduos que são maiores que $\frac{p}{2}$, então*

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

Demonstração. Sejam $r_1, r_2, \dots, r_n$ os inteiros maiores que $\frac{p}{2}$ no conjunto dos resíduos e $s_1, s_2, \dots, s_m$ aqueles menores que $\frac{p}{2}$. Sabemos que $n + m = \frac{p-1}{2}$.

Afirmamos que os números $(p - r_i)$ e (s_j) são todos distintos. Para uma contradição, suponha que para algum i, j , $p - r_i \equiv s_j \pmod{p}$. Então, $p - ha \equiv ga \pmod{p}$ para alguns $1 \leq h, g \leq \frac{p-1}{2}$, de modo que $-ha \equiv ga \pmod{p}$. Como $p \nmid a$, isso implica que $-h \equiv g \pmod{p}$, o que é impossível, pois $2 \leq g + h \leq p - 1$. Isso significa que os números $(p - r_i)$ e (s_j) formam uma permutação dos números $1, 2, \dots, \frac{p-1}{2}$.

Multiplicando esses números, obtemos que

$$\begin{aligned}
 \left(\frac{p-1}{2}\right)! &\equiv \prod_{i=1}^n (p - r_i) \prod_{j=1}^m s_j \\
 &\equiv (-r_1)(-r_2) \cdots (-r_n) s_1 s_2 \cdots s_m \\
 &\equiv (-1)^n r_1 r_2 \cdots r_n s_1 s_2 \cdots s_m \\
 &\equiv (-1)^n (a)(2a) \cdots \left(\frac{p-1}{2}a\right) \\
 &\equiv (-1)^n \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \pmod{p}.
 \end{aligned}$$

Como $\text{mdc}(p, \left(\frac{p-1}{2}\right)!) = 1$, temos que

$$(-1)^n a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

e, portanto,

$$(-1)^n \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

pelo Teorema 3.7.

□

Exemplo 3.22. Seja $p = 11$ e $a = 4$. Então $\text{mdc}(4, 11) = 1$ e $\frac{11-1}{2} = 5$. A tabela abaixo mostra os menores resíduos módulo 11 dos inteiros $a, 2a, \dots, 5a$.

	4	8	12	16	20
mod 11	4	8	1	5	9

Note que há três resíduos menores ou iguais a 5 e dois que são maiores que 5, então $n = 2$. Pelo Lema de Gauss, $\left(\frac{4}{11}\right) = (-1)^2 = 1$. Observe que a Propriedade 4 do símbolo de Legendre também nos dá esse resultado, pois 4 é um quadrado perfeito.

Usando o lema de Gauss, podemos agora provar o Teorema 3.23.

Teorema 3.23. *O número 2 é um resíduo quadrático de números primos da forma $8k + 1$ e $8k + 7$ e não é um resíduo quadrático de primos da forma $8k + 3$ e $8k + 5$. Esta informação pode ser resumida na fórmula*

$$(2/p) = (-1)^{(p^2-1)/8}.$$

Demonstração. A afirmação do teorema é equivalente a dizer que 2 é um resíduo quadrático (mod p) se p for da forma $8k \pm 1$ e um não-resíduo quadrático (mod p) se p for da forma $8k \pm 3$. Seja $F = \{2, 4, 6, 8, \dots, p-1\}$. Como p é um primo ímpar, então pode ser escrito como $p = 4k + 1$ ou $4k + 3$ para algum inteiro k .

Se $p = 4k + 1$, então $\{x \in F \mid x = sp + r, r > \frac{p}{2}\} = \{x \in F \mid x = \frac{p-1}{2} + 2m, m = 1, \dots, \frac{p-1}{4}\}$. Portanto,

$$\left(\frac{2}{p}\right) = (-1)^n \text{ onde } n = \frac{p-1}{4}.$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}} \begin{cases} 1, & \text{se } p = 8k + 1, \\ -1, & \text{se } p = 8k - 3. \end{cases}$$

Se $p = 4k + 3$, então $\{x \in F \mid x = \frac{p-1}{2} + 2m - 1\}$. Então $n = \frac{p+1}{4}$.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}} \begin{cases} 1, & \text{se } p = 8k - 1, \\ -1, & \text{se } p = 8k + 3. \end{cases}$$

Portanto,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Se $p = 8k \pm 1$, então

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

Então $\frac{p^2-1}{8}$ é par. Portanto,

$$(-1)^{\frac{p^2-1}{8}} = 1,$$

mas se $p = 8k \pm 3$, então

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

é ímpar. Assim,

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

□

Exemplo 3.24. Para ilustrar o Teorema 3.23, consideramos os primos 11, 13, 17 e 23. Como $11 \equiv 3 \pmod{8}$, ele tem a forma $8k + 3$. Pelo critério de Euler, (Teorema 3.7)

$$2^{(p-1)/2} = 2^{(11-1)/2} \equiv -1 \pmod{11},$$

portanto, $x^2 \equiv 2 \pmod{11}$ não tem solução e $(2/p) = -1$. A fórmula do Teorema 3.23 nos diz que

$$\begin{aligned} (-1)^{(p^2-1)/8} &= (-1)^{(11^2-1)/8} & (p = 11) \\ &= (-1)^{15} \\ &= -1 \end{aligned}$$

Da mesma forma, como $13 \equiv 5 \pmod{8}$, 13 tem a forma $8k + 5$, e

$$2^{(p-1)/2} = 2^6 \equiv -1 \pmod{13}.$$

Assim $(2/p) = -1$ e $(-1)^{(13^2-1)/8} = (-1)^{21} = -1$. Portanto 2 é um não-resíduo quadrático de 11 e 13, os quais são primos da forma $8k + 3$ e $8k + 5$, respectivamente.

Como $17 \equiv 1 \pmod{8}$, ele é da forma $8k + 1$, e

$$2^{(17-1)/2} = 2^8 = 256 \equiv 1 \pmod{17}.$$

Assim $x^2 \equiv 2 \pmod{17}$ tem uma solução, e $(2/p) = 1 = (-1)^{(17^2-1)/8}$.

Finalmente, $23 \equiv 7 \pmod{8}$, então 23 tem a forma $8k + 7$ e

$$2^{(23-1)/2} = 2^{11} = 2048 \equiv 1 \pmod{23},$$

e então $(2/p) = 1 = (-1)^{(23^2-1)/8}$. Portanto, 2 é um resíduo quadrático dos primos 17 e 23, os quais têm a forma $8k + 1$ e $8k + 7$, respectivamente.

Neste capítulo, exploramos o conceito fundamental de resíduos quadráticos e suas propriedades. No próximo capítulo, aprofundaremos nossa análise ao explorar as diferentes provas da Lei da Reciprocidade Quadrática.

4 Provas da Lei da Reciprocidade Quadrática

Além de Euler, a lei da reciprocidade quadrática também foi estudada por outros matemáticos, como Gauss em 1795 e Eisenstein em 1844. Embora seja verdade que Euler e Legendre iniciaram o estudo da reciprocidade quadrática, foi Gauss quem primeiro apresentou uma prova rigorosa. Ele eventualmente criou oito provas nas primeiras décadas do século XVIII e chamou-a de o “teorema dourado”. As principais referências usadas para o desenvolvimento deste capítulo foram [8, 13, 9, 16].

Teorema 4.1. *(Lei da Reciprocidade Quadrática) Sejam p e q primos ímpares distintos. Então:*

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

Um lema importante de que precisaremos nas provas da reciprocidade quadrática é o lema de Gauss (Lema 3.21).

Exemplo 4.2. Considere a congruência $x^2 \equiv 17471 \pmod{1697}$.

$$\begin{aligned} \left(\frac{17471}{1697}\right) &\equiv \left(\frac{501}{1697}\right) \pmod{1697} && \text{(Propriedade 3 do símbolo Legendre)} \\ &\equiv \left(\frac{3}{1697}\right)\left(\frac{167}{1697}\right) \pmod{1697} && \text{(Propriedade 2 do símbolo de Legendre)} \\ &\equiv \left(\frac{1697}{3}\right)\left(\frac{1697}{167}\right) \pmod{1697} && \text{(Lei da Reciprocidade Quadrática)} \\ &\equiv \left(\frac{2}{3}\right)\left(\frac{27}{167}\right) \pmod{1697} && \text{(Propriedade 3 do símbolo de Legendre)} \\ &\equiv \left(\frac{2}{3}\right)\left(\frac{3^2}{167}\right)\left(\frac{3}{167}\right) \pmod{1697} && \text{(Propriedade 2 do símbolo de Legendre)} \\ &\equiv (-1)^{(3^2-1)/8} \cdot (1) \cdot \left(-\left(\frac{167}{3}\right)\right) \pmod{1697} && \text{(Lei da Reciprocidade Quadrática)} \\ &\equiv (-1)(-1)\left(\frac{2}{3}\right) && \text{(Propriedade 3 do símbolo de Legendre)} \\ &\equiv (-1)^{(3^2-1)/8} \pmod{1697} && \text{(Lei da Reciprocidade Quadrática)} \\ &\equiv -1 \pmod{1697} && \text{(Aritmética)} \end{aligned}$$

Suponha que agora queiramos examinar $x^2 \equiv 1697 \pmod{17471}$ para ver se há uma solução. Certamente poderíamos repetir o processo acima para descobrir isso diretamente, mas esse método é bastante trabalhoso e há muitos lugares onde podem ocorrer erros aritméticos. É aqui que a Lei da Reciprocidade Quadrática nos auxilia. Nós sabemos que

$$\begin{aligned} \left(\frac{17471}{1697}\right) \left(\frac{1697}{17471}\right) &= (-1)^{(17471-1)(1697-1)/4} && \text{(Lei da Reciprocidade Quadrática)} \\ &= (-1)^{7407280} && \text{(Aritmética)} \\ &= 1, \end{aligned}$$

então ambos $\left(\frac{17471}{1697}\right)$ e $\left(\frac{1697}{17471}\right)$ são iguais a 1 ou ambos são iguais a -1. Como $\left(\frac{17471}{1697}\right) = -1$, segue que $\left(\frac{1697}{17471}\right) = -1$ também. Assim, pela definição do símbolo de Legendre (Definição 3.17), segue que 1697 não é um resíduo quadrático módulo 17471, isto é, $x^2 \equiv 1697 \pmod{17471}$ não possui solução.

Note que, pela definição Definição 3.17 17471 não é um resíduo quadrático módulo 1697, e portanto $x^2 \equiv 17471 \pmod{1697}$ também não possui solução.

4.1 Primeira prova: Usando o lema de Eisenstein

Nossa primeira prova da reciprocidade quadrática depende do lema de Gauss (Lema 3.21) e do lema de Eisenstein (Lema 4.3). Para mais informações sobre essa prova, veja [18].

Lembre-se de que $[x]$ é a função maior inteiro e $[x] \leq x < [x] + 1$. Usaremos esta função nas próximas provas.

Lema 4.3. (Lema de Eisenstein) *Se p e q são primos ímpares, então*

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor}.$$

Demonstração. Como na prova do lema de Gauss (Lema 3.21), consideramos os números $q, 2q, \dots, \frac{p-1}{2}q \pmod{p}$. Sejam $r_1, r_2, \dots, r_n$ os resíduos maiores que $\frac{p-1}{2}$ e $s_1, s_2, \dots, s_m$ os resíduos menores que $\frac{p-1}{2}$. Assim, $n + m = \frac{p-1}{2}$. Usando o algoritmo da divisão, encontramos que

$$kq = p \left\lfloor \frac{kq}{p} \right\rfloor + r,$$

onde r é o menor resíduo $\pmod{p}$ de kq . Se somarmos essas equações para k , obtemos

$$\sum_{k=1}^{\frac{p-1}{2}} kq = \sum_{k=1}^{\frac{p-1}{2}} p \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^n r_j + \sum_{j=1}^m s_j.$$

Temos

$$\sum_{k=1}^{\frac{p-1}{2}} k = 1 + 2 + \dots + \frac{p-1}{2} = \left(\frac{p-1}{2}\right) \left(\frac{p-1}{2} + 1\right) / 2$$

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

Portanto,

$$q \frac{p^2-1}{8} = p \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^n r_j + \sum_{j=1}^m s_j \quad (4.1)$$

$$q \frac{p^2-1}{8} = p \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^n (p - r_j) + \sum_{j=1}^m s_j. \quad (4.2)$$

Como os números $(p - r_j)$ e s_j formam uma permutação dos números $1, 2, \dots, \frac{p-1}{2}$, então

$$\frac{p^2-1}{8} = \sum_{j=1}^n (p - r_j) + \sum_{j=1}^m s_j = S + np - R. \quad (4.3)$$

Subtraindo (4.1) de (4.3), obtemos

$$(q-1) \frac{p^2-1}{8} = p \left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor - n \right) + 2R.$$

Note que p e q são primos ímpares, então o lado esquerdo é par e $2R$ é par. Assim, segue que

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor - n \text{ também é par.}$$

Portanto,

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor - n} = 1. \quad (4.4)$$

Por outro lado,

$$(-1)^n = \left(\frac{q}{p} \right) \quad (4.5)$$

pelo lema de Gauss (Lema 3.21). Portanto,

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor} = (-1)^n = \left(\frac{q}{p} \right), \quad (4.6)$$

como desejado. □

Exemplo 4.4. Seja $p = 11$ e $q = 7$. Então

$$\begin{aligned} \sum_{i=1}^{(11-1)/2} \left\lfloor \frac{7i}{11} \right\rfloor &= \left\lfloor \frac{7}{11} \right\rfloor + \left\lfloor \frac{14}{11} \right\rfloor + \left\lfloor \frac{21}{11} \right\rfloor + \left\lfloor \frac{28}{11} \right\rfloor + \left\lfloor \frac{35}{11} \right\rfloor \\ &= 0 + 1 + 1 + 2 + 3 \\ &= 7. \end{aligned}$$

Sabemos que

$$\begin{aligned} (7/11) &\equiv 7^{(11-1)/2} \pmod{11} \\ &\equiv 16807 \pmod{11} \\ &\equiv -1 \pmod{11}, \end{aligned}$$

e se aplicarmos o Lema 4.3, teremos $(7/11) = (-1)^7 = -1$.

Precisaremos também do seguinte lema.

Lema 4.5. *Se p e q são primos ímpares, então*

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor = \frac{(p-1)(q-1)}{4}. \quad (4.7)$$

Demonstração. A ideia principal da prova é que essa soma tem uma interpretação geométrica. Considere os pontos $A = (0, 0)$, $B = \left(\frac{p-1}{2}, 0\right)$, $C = \left(\frac{p-1}{2}, \frac{q-1}{2}\right)$, $D = \left(0, \frac{q-1}{2}\right)$. Então,

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$$

é o número de pontos de reticulado em $\mathbb{Z}^2$ ¹ contidos no interior do triângulo ABC . Além disso,

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$$

é o número de pontos de reticulado à esquerda da linha $AC = \frac{qx}{p}$ e contidos em ADC . Note que não há pontos inteiros na linha AC porque $\text{mdc}(p, q) = 1$. Assim, o número total de pontos no retângulo $ABCD$ é

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

□

Agora estamos em posição de provar a reciprocidade quadrática.

Demonstração. (Lei da Reciprocidade Quadrática) Do Lema 4.3, obtemos

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor} = \left(\frac{q}{p}\right). \quad (4.8)$$

Repetindo o argumento para $\left(\frac{p}{q}\right)$, obtemos

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor} = \left(\frac{p}{q}\right). \quad (4.9)$$

¹ Pontos de reticulado, ou pontos de rede, refere-se a um conjunto de pontos que formam uma grade ou malha em um espaço.

Multiplicando (4.8) e (4.9), encontramos que

$$\begin{aligned} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) &= (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor} (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor} \\ &= (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left(\left\lfloor \frac{kp}{q} \right\rfloor + \left\lfloor \frac{kq}{p} \right\rfloor \right)}, \end{aligned}$$

pelo Lema 4.3 (Lema de Eisenstein).

Portanto, pelo Lema 4.5 temos que

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

□

4.2 Segunda prova: Usando raízes da unidade

Nesta seção, provaremos nossa segunda prova da lei da reciprocidade quadrática. Essa prova foi publicada por Eisenstein em 1844. Para mais informações sobre essa prova, consulte a referência [17].

Lema 4.6. *Se n é um número inteiro ímpar, então*

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) \quad (4.10)$$

onde $\zeta = e^{\frac{2\pi i}{n}}$.

Demonstração. Note que $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ são todas as raízes n -ésimas de $z^n - 1$. Temos

$$z^n - 1 = \prod_{k=0}^{n-1} (z - \zeta^k).$$

Aplicando isso para $z = \frac{x}{y}$, temos

$$\frac{x^n}{y^n} - 1 = \prod_{k=0}^{n-1} \left(\frac{x}{y} - \zeta^k \right). \quad (4.11)$$

Multiplicando ambos os lados por y^n , temos

$$x^n - y^n = y^n \cdot \left(\prod_{k=0}^{n-1} \left(\frac{x}{y} - \zeta^k \right) \right).$$

Distribuindo o y^n dentro do produto, temos:

$$x^n - y^n = \prod_{k=0}^{n-1} \left(y \cdot \left(\frac{x}{y} - \zeta^k \right) \right) = \prod_{k=0}^{n-1} (x - \zeta^k y). \quad (4.12)$$

Como n é ímpar, quando k varia de 0 a $n-1$, $-2k$ forma um sistema completo de resíduos (mod n). Portanto,

$$x^n - y^n = \prod_{k=0}^{n-1} (x - \zeta^{-2k} y) \quad (4.13)$$

$$= \prod_{k=0}^{n-1} (x - \zeta^{-k} \cdot \zeta^{-k} y) \quad (4.14)$$

$$= \prod_{k=0}^{n-1} \left(x - \frac{\zeta^{-k}}{\zeta^k} y \right) \quad (4.15)$$

$$= \prod_{k=0}^{n-1} \left(\frac{\zeta^k x - \zeta^{-k} y}{\zeta^k} \right) \quad (4.16)$$

$$= \frac{\prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y)}{\prod_{k=0}^{n-1} \zeta^k} \quad (4.17)$$

$$= \frac{\prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y)}{\zeta^1 \cdot \zeta^2 \cdots \zeta^{n-1}} \quad (4.18)$$

$$= \zeta^{-1} \cdot \zeta^{-2} \cdots \zeta^{-(n-1)} \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y). \quad (4.19)$$

Como $-(1 + 2 + 3 + \cdots + (n-1)) = \frac{n(n-1)}{2}$ é divisível por n , temos

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y). \quad (4.20)$$

□

Para aprofundar a análise estrutural do produto

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y),$$

introduzimos a função

$$f(z) = e^{2\pi iz} - e^{-2\pi iz} = 2i \operatorname{sen}(2\pi z).$$

Cada fator do produto acima envolve pares conjugados do tipo ζ^k e ζ^{-k} , com $\zeta = e^{2\pi i/n}$, o que justifica a utilização de $f(z)$ como uma ferramenta analítica eficaz para reorganizar tais produtos. A função $f(z)$ é ímpar, periódica de período 1, e tem como únicos zeros reais os inteiros.

A Proposição 4.7, estabelece uma identidade para quocientes do tipo $f(nz)/f(z)$ como produtos indexados de translações da função f , permitindo fatorações simétricas em termos de $f\left(z \pm \frac{k}{n}\right)$.

Proposição 4.7. *Seja n um número inteiro ímpar. Então*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{\frac{n-1}{2}} \frac{f\left(z + \frac{k}{n}\right)}{f\left(z - \frac{k}{n}\right)}. \quad (4.21)$$

Demonstração. Seja $x = e^{2\pi iz}$ e $y = e^{-2\pi iz}$. Pelo Lema 4.6, temos

$$f(nz) = e^{2\pi inz} - e^{-2\pi inz} \quad (4.22)$$

$$= \prod_{k=0}^{n-1} \left(e^{2\pi iz} e^{\frac{2\pi ik}{n}} - e^{-2\pi iz} e^{-\frac{2\pi ik}{n}} \right) \quad (4.23)$$

$$= \prod_{k=0}^{n-1} \left(e^{\frac{2\pi i(k+nz)}{n}} - e^{\frac{-2\pi i(k+nz)}{n}} \right) \quad (4.24)$$

$$= \prod_{k=0}^{n-1} \left(e^{2\pi i\left(\frac{k}{n} + z\right)} - e^{-2\pi i\left(\frac{k}{n} + z\right)} \right) \quad (4.25)$$

$$= \prod_{k=0}^{n-1} f\left(\frac{k}{n} + z\right). \quad (4.26)$$

Quando k varia de $\frac{n+1}{2}$ até $n-1$, então $n-k$ varia de $\frac{n-1}{2}$ até 1. Portanto,

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{\frac{n-1}{2}} f\left(\frac{k}{n} + z\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(\frac{k}{n} + z\right). \quad (4.27)$$

Como f é periódica com período 1,

$$f\left(\frac{k}{n} + z\right) = f\left(\frac{k}{n} - 1 + z\right) = f\left(z - \frac{n-k}{n}\right).$$

Portanto,

$$\prod_{k=1}^{\frac{n-1}{2}} f\left(\frac{k}{n} + z\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(z - \frac{n-k}{n}\right) = \prod_{k=1}^{\frac{n-1}{2}} f\left(\frac{k}{n} + z\right) f\left(z - \frac{1+k}{n}\right).$$

Como $f(z+1) = f(z)$, temos

$$\prod_{k=1}^{\frac{n-1}{2}} f\left(\frac{k}{n} + z\right) f\left(z - \frac{1+k}{n}\right) = \prod_{k=1}^{\frac{n-1}{2}} f\left(\frac{k}{n} + z\right) f\left(z - \frac{k}{n}\right).$$

□

Proposição 4.8. *Seja $p \neq 2$ um número primo, $a \in \mathbb{Z}$ e $\text{mdc}(p, a) = 1$. Então*

$$\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}\right). \quad (4.28)$$

Demonstração. Seja $r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_m$ os menores resíduos de $a, 2a, 3a, \dots, \frac{p-1}{2}a$, onde, como na prova do lema de Gauss, $r_i > \frac{p-1}{2}$ e $s_i \leq \frac{p-1}{2}$. Para cada $1 \leq l \leq \frac{p-1}{2}$, seja

$$t_l \in \{p - r_1, p - r_2, \dots, p - r_n, s_1, \dots, s_m\}$$

o número único em $\{1, \dots, \frac{p-1}{2}\}$ tal que $\pm t_l \equiv la \pmod{p}$. Como f é periódica com período 1 e $f(-z) = -f(z)$, temos

$$f\left(\frac{la}{p}\right) = f\left(\pm \frac{t_l}{p}\right) = \pm f\left(\frac{t_l}{p}\right), \quad (4.29)$$

onde o sinal é + ou - dependendo se $t \in \{s_1, \dots, s_m\}$ ou $t_l \in \{p - r_1, p - r_2, \dots, p - r_n\}$. Multiplicando 4.29 sobre todos os $l \in \{1, \dots, \frac{p-1}{2}\}$, temos

$$\prod_{l=1}^{\frac{p-1}{2}} \pm f\left(\frac{t_l}{p}\right) \equiv \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{la}{p}\right). \quad (4.30)$$

À medida que l varia de 1 até $\frac{p-1}{2}$, t_l também varia de 1 até $\frac{p-1}{2}$. Pelo lema de Gauss (Lema 3.21), o número de sinais negativos em (4.30) é $(-1)^n = \left(\frac{a}{p}\right)$. Portanto,

$$\left(\frac{a}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}\right) = \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{la}{p}\right), \quad (4.31)$$

como desejado. $\square$

Demonstração. (Lei da Reciprocidade Quadrática) Agora podemos provar a lei da reciprocidade quadrática. Pela Proposição 4.8,

$$\left(\frac{q}{p}\right) = \prod_{l=1}^{\frac{p-1}{2}} \frac{f\left(\frac{lq}{p}\right)}{f\left(\frac{l}{p}\right)}. \quad (4.32)$$

Pela Proposição 4.7,

$$\frac{f\left(\frac{lq}{p}\right)}{f\left(\frac{l}{p}\right)} = \prod_{k=1}^{\frac{q-1}{2}} \frac{f\left(\frac{l}{p} + \frac{k}{q}\right)}{f\left(\frac{l}{p} - \frac{k}{q}\right)}. \quad (4.33)$$

Portanto,

$$\left(\frac{q}{p}\right) = \prod_{k=1}^{\frac{q-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} \frac{f\left(\frac{l}{p} + \frac{k}{q}\right)}{f\left(\frac{l}{p} - \frac{k}{q}\right)}. \quad (4.34)$$

Repetindo o argumento para $\left(\frac{p}{q}\right)$, obtemos

$$\left(\frac{p}{q}\right) = \prod_{k=1}^{\frac{q-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} \frac{f\left(\frac{k}{q} + \frac{l}{p}\right)}{f\left(\frac{k}{q} - \frac{l}{p}\right)}. \quad (4.35)$$

Como $f\left(\frac{k}{q} - \frac{l}{p}\right) = -f\left(\frac{l}{p} - \frac{k}{q}\right)$, concluímos que

$$\left(\frac{p}{q}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \left(\frac{q}{p}\right). \quad (4.36)$$

Portanto,

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}. \quad (4.37)$$

□

4.3 Terceira prova: Usando Teoria dos Grupos

Nossa terceira prova é devida a George Rousseau [19], em 1991. Ela não depende do lema de Gauss ou do lema de Eisenstein sobre pontos de reticulado. Esta prova baseia-se apenas no teorema de Wilson (Teorema 2.27), no critério de Euler (Teorema 3.7) e no teorema chinês dos restos (Teorema 2.42).

Como $(\mathbb{Z}/n\mathbb{Z})^*$ é o grupo multiplicativo dos inteiros módulo n . Sejam p, q primos, G/H o grupo quociente onde $G = (\mathbb{Z}/pq\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ e $H = \{\pm 1\} \cong \{(1, 1), (-1, -1)\}$ é um subgrupo normal de G . Determinamos o produto dos elementos de G/H multiplicando os representantes das classes laterais de H . Para mais informações sobre Teoria dos Grupos, consultar [14].

Dois resultados que são necessários na prova de Rousseau, o teorema de Wilson (Teorema 2.27) e o Lema 4.9, que é dado a seguir.

Lema 4.9. *Se p é um número primo, então*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p-1}{2}} (p-1)! \pmod{p}. \quad (4.38)$$

Demonstração. Para qualquer $1 \leq i \leq \frac{p-1}{2}$, temos $p-i \equiv -i \pmod{p}$. Portanto,

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

□

Agora apresentaremos a prova de Rousseau da reciprocidade quadrática.

Demonstração. (Teorema da Reciprocidade Quadrática) Pelo Teorema Chinês dos Restos (Teorema 2.42), temos uma função isomorfa

$$G = (\mathbb{Z}/pq\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*. \quad (4.39)$$

Qualquer elemento do grupo G pode ser representado na forma (a, b) , onde $a \in \{1, 2, \dots, p-1\}$ e $b \in \{1, 2, \dots, q-1\}$.

Considere o quociente de G pelo subgrupo $H = \{(1, 1), (-1, -1)\}$. Consideramos os representantes de G/H e tomamos seu produto π . Há duas maneiras de fazer isso. Primeiro, tomamos o conjunto completo de $(\mathbb{Z}/p\mathbb{Z})^*$ e a primeira metade de $(\mathbb{Z}/q\mathbb{Z})^*$. Então, uma lista de representantes de G/H é

$$\{(a, b) : 1 \leq a \leq p-1, 1 \leq b \leq \frac{q-1}{2}\}. \quad (4.40)$$

Como cada componente a é repetida $\frac{q-1}{2}$ vezes, o componente a de π é

$$(p-1)!^{\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}} \pmod{p} \quad (4.41)$$

pelo teorema de Wilson (Teorema 2.27). Cada componente b , $1, 2, \dots, \frac{q-1}{2}$, é repetida $p-1$ vezes. A componente b de π é

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

Portanto, o produto dos representantes é

$$\pi \equiv \left((-1)^{\frac{q-1}{2}} \pmod{p}, (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \pmod{q}\right). \quad (4.42)$$

Finalmente, escolhemos os representantes tomando a primeira metade de $(\mathbb{Z}/pq\mathbb{Z})^*$. Multiplicaremos todos os inteiros entre 1 e $\frac{pq-1}{2}$ que não são divisíveis por p ou q . Seja A o conjunto de inteiros em $[1, \frac{pq-1}{2}]$ que não são divisíveis por p . Os elementos de A são os seguintes:

$$\begin{aligned} &1, 2, 3, \dots, p-1, \\ &p+1, p+2, p+3, \dots, 2p-1, \\ &2p+1, 2p+2, 2p+3, \dots, 3p-1, \\ &\vdots \\ &\frac{q-1}{2}p+1, \frac{q-1}{2}p+2, \frac{q-1}{2}p+3, \dots, \frac{pq-1}{2}. \end{aligned}$$

Então $B = \{q, 2q, \dots, \frac{p-1}{2}q\}$ é o conjunto de todos os inteiros em A que são divisíveis por q . Assim, o componente a de π é

$$\begin{aligned} \prod_{n \in A, n \notin B} n &= \frac{\prod_{n \in A} n}{\prod_{n \in B} n} \\ &\equiv \frac{(p-1)!}{q^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!} \cdot q \cdot (2q) \cdot \dots \cdot \frac{p-1}{2} q \\ &\equiv \frac{(p-1)!}{q^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \left(\frac{p-1}{2}\right)! q^{\frac{p-1}{2}}} \\ &\equiv (-1)^{\frac{q-1}{2}} q^{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

Pelo critério de Euler (Teorema 3.7),

$$q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right) \pmod{p}. \quad (4.43)$$

Assim, o componente a de π é

$$\equiv (-1)^{\frac{q-1}{2}} q^{\frac{p-1}{2}} \pmod{p} = (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}. \quad (4.44)$$

De forma similar $\pmod{q}$, o componente b de π é

$$\equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}. \quad (4.45)$$

Portanto,

$$\pi = \left((-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}, (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q} \right). \quad (4.46)$$

Lembre-se que π é determinado até um fator de ± 1 . Comparando as duas expressões (4.42) e (4.46), obtemos

$$\begin{aligned} & \left((-1)^{\frac{q-1}{2}} \pmod{p}, (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \pmod{q} \right) = \\ & \pm \left((-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}, (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q} \right). \end{aligned}$$

Se o sinal for $+$, então

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

Se o sinal for $-$, então

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

Em qualquer caso,

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

□

As demonstrações da Lei da Reciprocidade Quadrática apresentadas neste capítulo, com o auxílio do Lema de Eisenstein, raízes da unidade e teoria dos grupos, em conjunto com as ferramentas da teoria dos números algébricos, estrutura multiplicativa do grupo das raízes da unidade e análise da estrutura multiplicativa de grupos finitos, respectivamente, proporcionou uma abordagem elegante e concisa para a prova da Lei da Reciprocidade Quadrática.

5 Aplicações

Resíduos quadráticos e a Lei da Reciprocidade Quadrática levaram a muitas aplicações diferentes em várias áreas. Concluímos o trabalho analisando algumas das aplicações mais comuns de resíduos quadráticos e da Lei da Reciprocidade Quadrática. Algumas dessas aplicações estão em criptografia, teoria dos grafos e teoria dos códigos. Além disso, serão apresentados exemplos implementados no SageMath, essas implementações permitirão visualizar propriedades fundamentais dos resíduos quadráticos e explorar aplicações diretas dos resultados teóricos discutidos. As principais referências usadas para o desenvolvimento deste capítulo foram [8, 13, 20, 21, 22, 23, 5, 6, 7].

5.1 Lei da Reciprocidade Quadrática em Criptografia

Com o crescimento da atividade digital, a criptografia tornou-se um campo de grande relevância, exigindo aprimoramento contínuo dos métodos empregados. O avanço tecnológico tem possibilitado o aumento da capacidade computacional, reduzindo, assim, o tempo necessário para resolver problemas considerados computacionalmente difíceis. Um dos fundamentos essenciais para diversos sistemas criptográficos consiste na resolução de congruências do tipo

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

onde n é um número composto. Este problema é notoriamente difícil de ser resolvido quando n é um número grande, sendo computacionalmente equivalente, em termos de complexidade, ao problema da fatoração de inteiros. Consequentemente, resíduos quadráticos desempenham um papel central em diversos protocolos criptográficos, como o sistema criptográfico de Rabin [2] e o esquema de transferência oblíqua (ou do inglês, *oblivious*) [24].

A fatoração de inteiros grandes constitui outro pilar fundamental sobre o qual diversos métodos criptográficos são construídos. No Volume VI de seu tratado *Disquisitiones Arithmeticae*, Gauss apresentou dois algoritmos distintos para fatoração, ambos baseados no conceito de resíduos quadráticos e na Lei da Reciprocidade Quadrática. Métodos modernos de fatoração, como o algoritmo da fração contínua, o algoritmo de Dixon e o crivo quadrático, mantêm a estrutura baseada em resíduos quadráticos e continuam a ser empregados na atualidade.

Paralelamente à fatoração de inteiros, destaca-se a área de testes de primalidade, que busca determinar de maneira eficiente se um dado número é primo. Dentre os diversos métodos

propostos, um dos mais notáveis é o teste de primalidade de Solovay-Strassen, que permite avaliar a primalidade de um número n . Além disso, um teste intimamente relacionado e amplamente utilizado é o teste de Miller-Rabin [4], que, embora inspirado na abordagem de Solovay-Strassen, apresenta maior confiabilidade e precisão. Embora o teste de Miller-Rabin não utilize diretamente a Lei da Reciprocidade Quadrática, ele se apoia no comportamento esperado dos resíduos quadráticos para identificar números compostos, sendo, portanto, um dos métodos probabilísticos mais eficientes para a verificação de primalidade.

A Tabela 5.1 apresenta alguns testes de primalidade, no entanto, existem muitos outros testes que foram desenvolvidos para diferentes aplicações.

Teste	Vantagens	Desvantagens
Solovay-Strassen	Rápido, baseado no símbolo de Jacobi	Pode falhar para pseudo-primos de Euler-Jacobi, menos eficiente que Miller-Rabin
Miller-Rabin	Mais confiável que Solovay-Strassen, amplamente utilizado	Ainda tem erro probabilístico
AKS	Garante primalidade, determinístico	Muito lento na prática para números grandes
Curvas Elípticas	Melhor para primos grandes, usado em aplicações criptográficas	Complexidade matemática maior
Teste de Lucas-Lehmer	Muito eficiente para números de Mersenne	Aplicável apenas a números de Mersenne
Teste de Fermat	Simples e rápido	Falsos positivos para números de Carmichael

Tabela 5.1: Comparação entre testes de primalidade

Os testes de Solovay-Strassen, Miller-Rabin, Fermat e Curvas Elípticas são testes probabilísticos. Por outro lado, os testes AKS e de Lucas-Lehmer são testes determinísticos.

Observação 5.1. O Teste de Rabin não foi apresentado na Tabela 5.1, pois ele não é um teste usado para testar a primalidade de um número. Ele é usado para fatorar números compostos, ajudando a quebrar criptografia baseada em fatoração.

5.1.1 Aplicação 1: Teste de Miller–Rabin

O *Teste de Miller–Rabin* é um *teste probabilístico* que verifica se um número n é primo, baseando-se no comportamento esperado da exponenciação modular segundo o *Pequeno Teorema de Fermat* e propriedades de resíduos quadráticos.

A seguir, descrevemos formalmente as etapas do teste:

1. Verificar casos triviais.

Se $n = 2$ ou $n = 3$, então n é primo. Se n for par e maior que 2, então n é composto.

2. Escrever $n - 1$ na forma $d \cdot 2^s$, com d ímpar.

Isto é, encontrar inteiros $s \geq 1$ e d ímpar tais que

$$n - 1 = 2^s \cdot d.$$

3. Escolher uma base aleatória a , com $2 \leq a \leq n - 2$ e $\text{mdc}(a, n) = 1$.**4. Calcular $x \equiv a^d \pmod{n}$.**

Se $x \equiv 1 \pmod{n}$ ou $x \equiv -1 \pmod{n}$, então n pode ser primo, e passamos para outra base a .

5. Realizar até $s - 1$ iterações quadráticas:

Para $r = 1, \dots, s - 1$, computar

$$x \equiv x^2 \pmod{n}.$$

Se em alguma iteração encontrarmos $x \equiv -1 \pmod{n}$, encerramos a sequência e testamos outra base a .

Caso contrário, se após todas as iterações tivermos $x \not\equiv -1 \pmod{n}$, então n é *composto*.

6. Repetir o teste para outras bases a .

O teste é repetido para k bases aleatórias a . Se em alguma das iterações o número n for identificado como composto, então ele é definitivamente composto.

Se n passar em todas as k iterações, então dizemos que n é *provavelmente primo*.

Esse teste é mais confiável do que o Teste de Fermat e é amplamente utilizado em algoritmos criptográficos para geração de grandes números primos com alta confiança.

Exemplo 5.2. Vamos verificar se $n = 61$ é primo utilizando o Teste de Miller–Rabin.

1. Verificação de casos triviais. Como $n = 61$ é ímpar e maior que 3, passamos para as etapas seguintes.

2. Escrever $n - 1$ na forma $d \cdot 2^s$.

$$n - 1 = 61 - 1 = 60 = 15 \cdot 2^2,$$

portanto:

$$d = 15, \quad s = 2.$$

3. Escolha da base. Tomamos $a = 2$, que pertence ao intervalo $2 \leq a \leq n - 2 = 59$ e satisfaz $\text{mdc}(a, n) = 1$.

4. **Cálculo de $x \equiv a^d \pmod{n}$.** Vamos calcular $x \equiv 2^{15} \pmod{61}$ por exponenciação modular:

$$\begin{aligned} 2^5 &= 32, \\ 2^{10} &= (2^5)^2 = 32^2 = 1024 \equiv 47 \pmod{61}, \\ 2^{15} &= 2^{10} \cdot 2^5 \equiv 47 \cdot 32 = 1504 \equiv 32 \pmod{61}. \end{aligned}$$

Como $x \equiv 32 \not\equiv \pm 1 \pmod{61}$, seguimos para as iterações.

5. **Iterações quadráticas (até $s - 1 = 1$ vez).** Calculamos:

$$x \equiv 32^2 = 1024 \equiv 47 \pmod{61}.$$

Como $x \not\equiv -1 \pmod{61}$, testamos uma nova base.

6. **Nova base: $a = 7$.** Calculamos $x \equiv 7^{15} \pmod{61}$:

$$\begin{aligned} 7^5 &= 16807 \equiv 49 \pmod{61}, \\ 7^{10} &= (7^5)^2 = 49^2 = 2401 \equiv 4 \pmod{61}, \\ 7^{15} &= 7^{10} \cdot 7^5 \equiv 4 \cdot 49 = 196 \equiv 13 \pmod{61}. \end{aligned}$$

Como $x \equiv 13 \not\equiv \pm 1 \pmod{61}$, prosseguimos com a iteração:

$$x \equiv 13^2 = 169 \equiv 47 \pmod{61}.$$

Ainda temos $x \not\equiv -1 \pmod{61}$, portanto n não foi classificado como primo com base nas escolhas de $a = 2$ e $a = 7$.

7. **Conclusão.** Como em nenhuma das bases $a = 2$ e $a = 7$ o valor x foi congruente a $-1 \pmod{n}$ em alguma iteração, e tampouco $x \equiv 1 \pmod{n}$ inicialmente, o número $n = 61$ ainda não pode ser classificado como primo com certeza. Contudo, novos testes com outras bases poderiam confirmar a provável primalidade de n . De fato, 61 é primo, e o teste com mais bases confirmaria isso com alta probabilidade.

Observação 5.3. Para um número pequeno como 61, podemos verificar diretamente que ele é de fato primo. No entanto, para números grandes, o Teste de Miller-Rabin não dá certeza absoluta, apenas reduz a probabilidade de erro. Para números grandes usados em criptografia, esse teste é amplamente usado porque a probabilidade de erro pode ser reduzida a níveis insignificantes ao escolher muitas bases aleatórias.

5.1.2 Exemplo usando Sagemath

Vamos agora apresentar uma implementação do Exemplo 5.2 no software livre SageMath.

```
1 def miller_rabin_test(n, a):
2     """
3     Aplica o teste de Miller-Rabin para um número n e uma base a.
4     Retorna True se n for provavelmente primo, False se for composto.
5     """
6     if n < 2:
7         return False
8     if n in [2, 3]:
9         return True
10    if n % 2 == 0:
11        return False
12
13    # Escrever n - 1 como d * 2^s
14    d, s = n - 1, 0
15    while d % 2 == 0:
16        d //= 2
17        s += 1
18
19    # Computar x = a^d mod n
20    x = pow(a, d, n)
21    if x == 1 or x == n - 1:
22        return True
23
24    # Elevar ao quadrado até s-1 vezes
25    for _ in range(s - 1):
26        x = pow(x, 2, n)
27        if x == n - 1:
28            return True
29
30    return False # Se nenhum dos critérios foi satisfeito, n é composto
31
32    #Testando para n=61 com todas as bases 2<=a <= n-2 e mdc(a,n) = 1
33    n = 61
34    bases = [a for a in range(2, n - 1) if gcd(a, n) == 1]
35
36    resultados = {a: miller_rabin_test(n, a) for a in bases}
37
38    # Exibir os resultados em 3 colunas
39    colunas = 3
40    linhas = -(-len(resultados) // colunas)
41    resultado_lista = list(resultados.items())
42
43    for i in range(linhas):
44        linha = ""
45        for j in range(colunas):
```

```

46     index = i + j * linhas
47     if index < len(resultado_lista):
48         base, resultado = resultado_lista[index]
49         linha += f"Base_{base}:_{n}_é primo?_{resultado}\t"
50     print(linha)

```

Como resultado dessa implementação no Sagemath, obtemos a resposta:

Base 2: 61 é primo? True	Base 22: 61 é primo? True	Base 42: 61 é primo? True
Base 3: 61 é primo? True	Base 23: 61 é primo? True	Base 43: 61 é primo? True
Base 4: 61 é primo? True	Base 24: 61 é primo? True	Base 44: 61 é primo? True
Base 5: 61 é primo? True	Base 25: 61 é primo? True	Base 45: 61 é primo? True
Base 6: 61 é primo? True	Base 26: 61 é primo? True	Base 46: 61 é primo? True
Base 7: 61 é primo? True	Base 27: 61 é primo? True	Base 47: 61 é primo? True
Base 8: 61 é primo? True	Base 28: 61 é primo? True	Base 48: 61 é primo? True
Base 9: 61 é primo? True	Base 29: 61 é primo? True	Base 49: 61 é primo? True
Base 10: 61 é primo? True	Base 30: 61 é primo? True	Base 50: 61 é primo? True
Base 11: 61 é primo? True	Base 31: 61 é primo? True	Base 51: 61 é primo? True
Base 12: 61 é primo? True	Base 32: 61 é primo? True	Base 52: 61 é primo? True
Base 13: 61 é primo? True	Base 33: 61 é primo? True	Base 53: 61 é primo? True
Base 14: 61 é primo? True	Base 34: 61 é primo? True	Base 54: 61 é primo? True
Base 15: 61 é primo? True	Base 35: 61 é primo? True	Base 55: 61 é primo? True
Base 16: 61 é primo? True	Base 36: 61 é primo? True	Base 56: 61 é primo? True
Base 17: 61 é primo? True	Base 37: 61 é primo? True	Base 57: 61 é primo? True
Base 18: 61 é primo? True	Base 38: 61 é primo? True	Base 58: 61 é primo? True
Base 19: 61 é primo? True	Base 39: 61 é primo? True	Base 59: 61 é primo? True
Base 20: 61 é primo? True	Base 40: 61 é primo? True	
Base 21: 61 é primo? True	Base 41: 61 é primo? True	

[]:

5.1.3 Aplicação 2: Sistema Criptográfico de Rabin.

O sistema criptográfico de Rabin é semelhante ao RSA, pois baseado no problema da fatoração de inteiros, mas sua segurança se baseia na dificuldade de resolver a congruência quadrática $x^2 \equiv c \pmod{n}$, onde n é um produto de dois grandes números primos. A encriptação é simples, envolvendo apenas uma operação de exponenciação modular.

O sistema criptográfico de Rabin é considerado probabilístico, pois incorpora um elemento de aleatoriedade durante o processo de cifragem, o que pode resultar em mensagens cifradas distintas a cada execução. Em contraste, o sistema RSA é determinístico, produzindo sempre a mesma mensagem cifrada a partir de uma dada entrada e chave.

A Lei da Reciprocidade Quadrática ajuda a analisar os resíduos quadráticos e a determinar a existência de soluções para congruências quadráticas. Isso é crucial para entender a criptografia de Rabin, pois permite a verificação de quais números são resíduos quadráticos módulo n .

A seguir, apresentamos as etapas do Sistema Criptográfico de Rabin.

1. Configuração do Sistema

- (a) Escolha dois números primos distintos p e q .
- (b) Calcule $n = p \cdot q$. Este valor n será a chave pública do sistema, enquanto p e q serão mantidos em segredo como chave privada.

2. Encriptação

- (a) Mensagem: Representar a mensagem m como um número inteiro $0 \leq m < n$.
- (b) Texto cifrado: A mensagem é cifrada utilizando a fórmula:

$$c \equiv m^2 \pmod{n}.$$

O valor c é o texto cifrado.

3. Decriptação

- (a) Resolver a congruência quadrática: Dado o texto cifrado c , resolver a congruência:

$$x^2 \equiv c \pmod{n}.$$

Para isso:

- Divida n em seus fatores primos p e q .
- Resolva as congruências quadráticas $x^2 \equiv c \pmod{p}$ e $x^2 \equiv c \pmod{q}$ separadamente.

Isso resulta em duas soluções x_1, x_2 módulo p e y_1, y_2 módulo q . Combine as 4 combinações possíveis de (x, y) usando o Teorema Chinês do Resto (TCR) (Teorema 2.42) para encontrar as soluções z módulo n :

$$z \equiv x \pmod{p}, \quad z \equiv y \pmod{q}.$$

Use o TCR para calcular os valores de z .

4. Seleção da Mensagem Original

- (a) As soluções obtidas do TCR representam as possíveis mensagens m .
- (b) Use o contexto para identificar a mensagem original entre as soluções.

O sistema criptográfico de Rabin apresenta vantagens em termos de segurança, pois a dificuldade de resolver a congruência quadrática $x^2 \equiv c \pmod{n}$ está diretamente relacionada ao problema da fatoração de inteiros. No entanto, a ambiguidade gerada durante a decriptação, devido às múltiplas soluções, é uma desvantagem importante. A adoção de mecanismos adicionais, como redundância ou restrição de intervalo, é essencial para garantir a correta identificação da mensagem original.

Exemplo 5.4. De acordo com as etapas anteriores, apresentamos um exemplo do sistema criptográfico de Rabin.

1. Configuração do Sistema

- (a) Escolha dois números primos distintos $p = 7$ e $q = 11$.

(b) Calcule $n = p \cdot q = 7 \cdot 11 = 77$.

2. Encriptação

(a) Vamos escolher $m = 5$. A mensagem é cifrada utilizando a fórmula.

$$c \equiv m^2 \pmod{n}.$$

Substituindo os valores temos:

$$c \equiv 5^2 \pmod{77} \Rightarrow c \equiv 25 \pmod{77}.$$

Logo, o texto cifrado é $c = 25$.

3. Decriptação

(a) Dado o texto cifrado $c = 25$, vamos resolver a congruência quadrática

$$x^2 \equiv 25 \pmod{77}.$$

Para isso vamos dividir $n = 77$ em seus fatores primos $p = 7$ e $q = 11$ e vamos resolver as congruências quadráticas separadamente: Como $25 \equiv 4 \pmod{7}$ vamos resolver $x^2 \equiv 4 \pmod{7}$. As soluções são:

$$x \equiv 2 \pmod{7} \text{ e } x \equiv 5 \pmod{7}.$$

Agora, como $25 \equiv 3 \pmod{11}$ vamos resolver $y^2 \equiv 3 \pmod{11}$. As soluções são:

$$y \equiv 5 \pmod{11} \text{ e } y \equiv 6 \pmod{11}.$$

Agora, tomando as 4 combinações possíveis de (x, y) usando o Teorema Chinês do Resto (TCR) temos:

$$z \equiv x \pmod{p}, \quad z \equiv y \pmod{q}.$$

e com isso, as combinações são:

$$(x_1, y_1) = (2, 5), (x_1, y_2) = (2, 6), (x_2, y_1) = (5, 5), (x_2, y_2) = (5, 6).$$

Para cada combinação:

- Para $(x, y) = (2, 5)$:

$$z = (2 \cdot 11 \cdot 2) + (5 \cdot 7 \cdot 8) \pmod{77} = 16.$$

- Para $(x, y) = (2, 6)$:

$$z = (2 \cdot 11 \cdot 2) + (6 \cdot 7 \cdot 8) \pmod{77} = 72.$$

- Para $(x, y) = (5, 5)$:

$$z = (5 \cdot 11 \cdot 2) + (5 \cdot 7 \cdot 8) \pmod{77} = 5.$$

- Para $(x, y) = (5, 6)$:

$$z = (5 \cdot 11 \cdot 2) + (6 \cdot 7 \cdot 8) \pmod{77} = 61.$$

4. Seleção da Mensagem Original As soluções obtidas do TCR são:

$$z = \{16, 72, 5, 61\}.$$

Como não colocamos nenhum mecanismo adicional, não é possível identificar a mensagem original. No entanto, podemos restringir m a um intervalo específico, por exemplo, $0 \leq m < \sqrt{n}$, de forma que apenas uma solução pertença a esse intervalo.

No exemplo acima, se colocarmos a restrição de que a mensagem original m estará no intervalo $0 \leq m < \sqrt{77}$, então como $\sqrt{77} \approx 8.77$, restringimos m para o intervalo $0 \leq m < 8$. Com essa restrição, dentre as soluções $z = \{16, 72, 5, 61\}$, apenas $z = 5$ está dentro do intervalo permitido. Assim, identificamos que a mensagem original é $m = 5$.

5.1.4 Exemplo usando SageMath

A seguir, vamos apresentar uma implementação do Exemplo 5.4 do sistema criptográfico de Rabin utilizando o software livre *SageMath*.

```

1  # Configuração do Sistema
2  p = 7  # Primeiro número primo
3  q = 11 # Segundo número primo
4  n = p * q  # Chave pública
5
6  # Encriptação
7  m = 5  # Mensagem original
8  c = (m^2) % n  # Cálculo do texto cifrado
9  print(f"Texto cifrado {c}: {c}")
10
11 # Decriptação
12 # Resolver as congruências quadráticas separadamente
13 var('x')  # Declarar x como variável simbólica
14
15 # Modulo p
16 c_mod_p = c % p
17 solutions_p = solve_mod(x^2 == c_mod_p, p)
18 print(f"Raízes módulo p ({p}): {solutions_p}")
19
20 # Modulo q
21 c_mod_q = c % q
22 solutions_q = solve_mod(x^2 == c_mod_q, q)

```

```

23 print(f"Raízes_módulo_q({q}):_{solutions_q}")
24
25 # Combinações possíveis de (x, y)
26 from itertools import product
27 combinations = list(product(solutions_p, solutions_q))
28 print(f"Combinações possíveis de (x, y):_{combinations}")
29
30 # Teorema Chinês do Resto (TCR)
31 def crt(x, y, p, q):
32     n = p * q
33     q_inv = inverse_mod(q, p)
34     p_inv = inverse_mod(p, q)
35     z = (x * q * q_inv + y * p * p_inv) % n
36     return z
37
38 # Calcular todas as combinações com TCR
39 solutions = []
40 for x_tuple, y_tuple in combinations:
41     x = x_tuple[0] # Extrai o valor da tupla
42     y = y_tuple[0] # Extrai o valor da tupla
43     z = crt(Integer(x), Integer(y), p, q) # Agora x e y são inteiros
44     solutions.append(z)
45     print(f"Combinação (x, y) = ({x}, {y}) => z = {z}")
46
47 # Resultado final
48 print(f"Possíveis mensagens decifradas:_{solutions}")
49
50 # Identificar a mensagem original
51 if m in solutions:
52     print(f"A mensagem original é:_{m}")
53 else:
54     print("Mensagem original não encontrada nas soluções.")

```

Executando o código a partir dos dados do Exemplo 5.4 no SageMath, obtemos como resposta:

```

Texto cifrado (c): 25
Raízes módulo p (7): [(2,), (5,)]
Raízes módulo q (11): [(5,), (6,)]
Combinações possíveis de (x, y): [((2,), (5,)), ((2,), (6,)), ((5,), (5,)), ((5,), (6,))]
Combinação (x, y) = (2, 5) => z = 16
Combinação (x, y) = (2, 6) => z = 72
Combinação (x, y) = (5, 5) => z = 5
Combinação (x, y) = (5, 6) => z = 61
Possíveis mensagens decifradas: [16, 72, 5, 61]
A mensagem original é: 5

```

[]:

A mensagem original $m = 5$ está entre os valores decifrados, confirmando o procedimento.

5.1.5 Aplicação 3: Teste de Primalidade de Solovay-Strassen

O teste de primalidade de Solovay-Strassen é um teste probabilístico que verifica a primalidade de um número usando propriedades de resíduos quadráticos. A referência clássica para o Teste de Primalidade de Solovay-Strassen é [3]. Embora tenha sido um avanço significativo na época, foi posteriormente superado pelo Teste de Miller-Rabin, que é mais eficiente e confiável. O teste verifica a congruência $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$, onde $\left(\frac{a}{n}\right)$ é o símbolo de Jacobi, uma generalização do símbolo de Legendre. Utilizamos a Lei da Reciprocidade Quadrática para calcular o símbolo de Jacobi e verificar a congruência.

A seguir, apresentamos as etapas do teste.

1. Escolha um número n a ser testado.
2. Selecione um número a aleatório tal que $1 < a < n - 1$.
3. Calcule $a^{(n-1)/2} \pmod{n}$.
4. Calcule o símbolo de Jacobi $\left(\frac{a}{n}\right)$ usando a Lei da Reciprocidade Quadrática.
5. Verifique se $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$. Se a congruência não for satisfeita, então n é composto.

Exemplo 5.5. Vamos determinar a primalidade de $n = 561$, utilizando o teste de Solovay-Strassen. Para este exemplo, escolhemos $a = 2$, com $1 < a < n - 1$.

Inicialmente, calculamos o símbolo de Jacobi $\left(\frac{2}{561}\right)$. Como $561 = 3 \cdot 11 \cdot 17$, podemos decompô-lo como:

$$\left(\frac{2}{561}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{11}\right) \cdot \left(\frac{2}{17}\right).$$

Para cada termo, aplicamos as propriedades do símbolo de Jacobi. Para o primeiro fator, $\left(\frac{2}{3}\right) = -1$, pois $2 \equiv -1 \pmod{3}$ e -1 é um resíduo não-quadrático módulo 3. Para o segundo fator, $\left(\frac{2}{11}\right) = 1$, pois 2 é um resíduo quadrático módulo 11. Para o terceiro fator, $\left(\frac{2}{17}\right) = -1$, uma vez que $2 \equiv -1 \pmod{17}$, e -1 não é um resíduo quadrático módulo 17. Multiplicando os resultados, temos:

$$\left(\frac{2}{561}\right) = (-1) \cdot 1 \cdot (-1) = 1.$$

Em seguida, calculamos $2^{(n-1)/2} \pmod{n}$, ou seja, $2^{280} \pmod{561}$. Calculamos sucessivamente os valores intermediários:

$$2^2 \equiv 4 \pmod{561}, \quad 2^4 \equiv 16 \pmod{561}, \quad 2^8 \equiv 256 \pmod{561}, \quad 2^{16} \equiv 460 \pmod{561}.$$

Continuando o processo até 2^{280} , obtemos:

$$2^{280} \equiv 263 \pmod{561}.$$

Agora, verificamos a congruência estabelecida pelo teste:

$$2^{280} \equiv \left(\frac{2}{561}\right) \pmod{561}.$$

Substituindo os valores calculados, temos $263 \not\equiv 1 \pmod{561}$, ou seja, a congruência falha, o que implica que $n = 561$ é composto. Portanto, concluímos que o número $n = 561$ não é primo.

5.1.6 Exemplo usando Sagemath

Vamos agora apresentar uma implementação do Exemplo 5.5 no software livre SageMath.

```

1
2 import random
3
4 def jacobi(a, n):
5     """
6     Calcula o símbolo de Jacobi (a/n).
7     :param a: Inteiro a
8     :param n: Inteiro ímpar positivo
9     :return: -1, 0 ou 1
10    """
11    if n <= 0 or n % 2 == 0:
12        raise ValueError("n deve ser um número ímpar positivo.")
13
14    a = a % n
15    result = 1
16
17    while a != 0:
18        while a % 2 == 0:
19            a //= 2
20            if n % 8 in [3, 5]:
21                result = -result
22
23        a, n = n, a # Lei da reciprocidade quadrática
24        if a % 4 == n % 4 == 3:
25            result = -result
26        a %= n
27
28    return result if n == 1 else 0
29
30 def solovay_strassen(n, k=10):
31     """
32     Teste de primalidade de Solovay-Strassen para um número n.
33     :param n: Número a ser testado
34     :param k: Número de iterações do teste probabilístico
35     :return: True se n for provavelmente primo, False se for composto
36    """

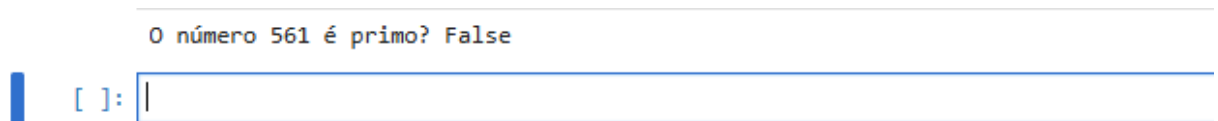
```

```

37     if n < 2:
38         return False
39     if n in [2, 3]:
40         return True
41     if n % 2 == 0:
42         return False
43
44     for _ in range(k):
45         a = random.randint(2, n - 2)
46         exp = (n - 1) // 2
47         jacobi_symbol = jacobi(a, n) % n
48         mod_exp = pow(a, exp, n) # Cálculo modular de a^((n-1)/2) % n
49
50         if jacobi_symbol != mod_exp:
51             return False # n é composto
52
53     return True # n é provavelmente primo
54
55     # Exemplo com n=561 (conhecido como pseudoprimo para alguns testes)
56 n = 561
57 print(f"O número {n} é primo? {solovay_strassen(n)}")

```

Executando o código acima no SageMath, obtemos:



O número 561 é primo? False

[]: |

5.2 Lei da Reciprocidade Quadrática em Teoria dos Grafos

Existem certos tipos de grafos na teoria dos grafos que são chamados de grafos de Paley, que têm ligações com resíduos quadráticos. Grafos de Paley são grafos não direcionados que são construídos a partir de elementos de um campo finito que diferem apenas por um resíduo quadrático. O estudo desses grafos levou ao desenvolvimento de algo chamado construção de Paley, que é usada para criar matrizes de Hadamard a partir de resíduos quadráticos. Essas matrizes têm sido estudadas extensivamente, pois possuem muitas propriedades interessantes que fascinam os matemáticos.

Vamos explorar um exemplo de como a Lei da Reciprocidade Quadrática pode ser utilizada na teoria dos grafos, especificamente na construção de um grafo de Paley.

5.2.1 Aplicação: Grafos de Paley

Um grafo de Paley é um tipo de grafo não direcionado que é construído a partir dos elementos de um corpo finito $\mathbb{F}_q$ onde q é um número primo congruente a 1 módulo 4. Os vértices do

grafo correspondem aos elementos do corpo finito, e dois vértices x e y estão conectados por uma aresta se $x - y$ é um resíduo quadrático em $\mathbb{F}_q$.

Exemplo 5.6. Neste exemplo, construímos o grafo de Paley P_5 para $q = 5$, onde q é um número primo congruente a 1 (mod 4). Este grafo é definido sobre o corpo finito $\mathbb{F}_5$, que contém os elementos $\{0, 1, 2, 3, 4\}$. O grafo é construído conectando dois vértices x e y se $x - y$ for um resíduo quadrático em $\mathbb{F}_5$.

Primeiramente, identificamos os elementos de $\mathbb{F}_5$ e determinamos os resíduos quadráticos neste corpo finito. Os elementos de $\mathbb{F}_5$ são os inteiros $\{0, 1, 2, 3, 4\}$, com as operações de adição e multiplicação definidas módulo 5. Para encontrar os resíduos quadráticos, calculamos $x^2 \pmod{5}$ para cada elemento $x \in \mathbb{F}_5 \setminus \{0\}$. Os resultados são os seguintes:

$$1^2 \equiv 1 \pmod{5}, \quad 2^2 \equiv 4 \pmod{5}, \quad 3^2 \equiv 9 \equiv 4 \pmod{5}, \quad 4^2 \equiv 16 \equiv 1 \pmod{5}.$$

Observamos que os resíduos quadráticos em $\mathbb{F}_5$ são $\{1, 4\}$, enquanto 0 não é considerado um resíduo quadrático.

Agora, construímos o grafo de Paley P_5 . Os vértices do grafo correspondem aos elementos $\{0, 1, 2, 3, 4\}$. Dois vértices x e y estão conectados por uma aresta se $x - y \in \{1, 4\} \pmod{5}$. Este critério é aplicado de forma sistemática para determinar as conexões entre os vértices:

- $x = 0$:
 - $0 - 1 = -1 \equiv 4 \pmod{5} \Rightarrow$ conecta com 1
 - $0 - 4 = -4 \equiv 1 \pmod{5} \Rightarrow$ conecta com 4
- $x = 1$:
 - $1 - 0 \equiv 1 \pmod{5} \Rightarrow$ conecta com 0
 - $1 - 2 = -1 \equiv 4 \pmod{5} \Rightarrow$ conecta com 2
- $x = 2$:
 - $2 - 1 \equiv 1 \pmod{5} \Rightarrow$ conecta com 1
 - $2 - 3 = -1 \equiv 4 \pmod{5} \Rightarrow$ conecta com 3
- $x = 3$:
 - $3 - 2 \equiv 1 \pmod{5} \Rightarrow$ conecta com 2
 - $3 - 4 = -1 \equiv 4 \pmod{5} \Rightarrow$ conecta com 4
- $x = 4$:
 - $4 - 0 \equiv 4 \pmod{5} \Rightarrow$ conecta com 0
 - $4 - 3 \equiv 1 \pmod{5} \Rightarrow$ conecta com 3

Visualmente, o grafo P_5 pode ser representado como um grafo não-direcionado com 5 vértices e arestas conectando os pares indicados acima.

5.2.2 Exemplo usando Sagemath

Vamos agora apresentar uma implementação do Exemplo 5.6 no software livre SageMath.

```

1
2 # Definir o corpo finito
3 q = 5
4 F = FiniteField(q)
5
6 # Encontrar os resíduos quadráticos
7 residuos_quadraticos = {x^2 % q for x in range(q)}
8 print(f"Resíduos quadráticos em F_{q}: {residuos_quadraticos}")
9
10 # Construir o grafo de Paley
11 G = Graph()
12 for x in range(q):
13     G.add_vertex(x)
14     for y in range(q):
15         if x != y and (x - y) % q in residuos_quadraticos:
16             G.add_edge(x, y)
17
18 # Desenhar o grafo
19 G.show()

```

Executando o código acima no SageMath, obtemos a seguinte visualização do Grafo de Paley P_5 :

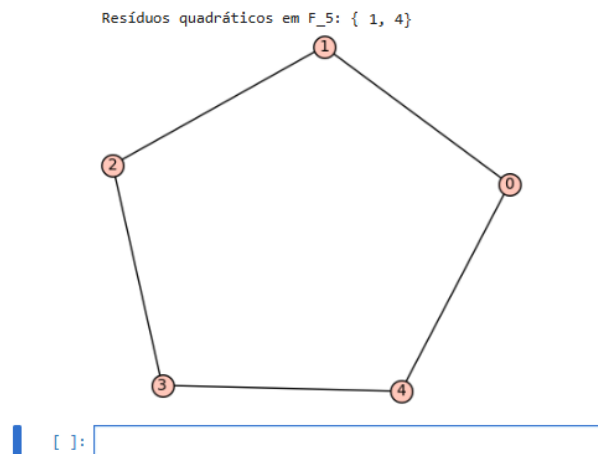


Figura 5.1: Grafo de Paley P_5 com $q = 5$.

Fonte: Elaborada pelo autor no Sagemath.

5.3 Lei da Reciprocidade Quadrática em Teoria dos Códigos

A Lei da Reciprocidade Quadrática pode ser aplicada na teoria dos códigos, especialmente na construção de códigos cíclicos, que são usados em sistemas de comunicação para detectar e corrigir erros.

5.3.1 Aplicação: Teoria dos Códigos Cíclicos

Um código cíclico C de comprimento n sobre um corpo finito $\mathbb{F}_q$ é um subespaço linear de $\mathbb{F}_q^n$ tal que, para cada vetor $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in C$, o vetor $\mathbf{c}' = (c_{n-1}, c_0, c_1, \dots, c_{n-2})$ (uma permutação cíclica de $\mathbf{c}$) também pertence a C .

Os códigos cíclicos são uma classe importante de códigos lineares que têm a propriedade cíclica: se uma palavra-código $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$ pertence ao código, então qualquer permutação cíclica de $\mathbf{c}$ também pertence ao código. Eles são amplamente utilizados em sistemas de comunicação e armazenamento de dados devido à sua capacidade de detectar e corrigir erros.

A propriedade cíclica dos códigos cíclicos é convenientemente representada usando polinômios. Cada vetor $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$ em $\mathbb{F}_q^n$ pode ser associado a um polinômio

$$c(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x].$$

A operação de permutação cíclica corresponde à multiplicação do polinômio $c(x)$ por x módulo $x^n - 1$. Formalmente, essa operação pode ser definida pela seguinte função:

$$\begin{aligned} T : \mathbb{F}_q[x] &\longrightarrow \mathbb{F}_q[x]/(x^n - 1) \\ c(x) &\longmapsto (x \cdot c(x)) \pmod{(x^n - 1)}. \end{aligned}$$

Um código cíclico C pode ser completamente descrito por um único polinômio gerador $g(x)$ que divide $x^n - 1$. O código C consiste em todos os múltiplos de $g(x)$:

$$C = \{c(x) = g(x)q(x) \mid q(x) \in \mathbb{F}_q[x], \deg(c(x)) < n\}.$$

O polinômio gerador $g(x)$ deve ser um divisor de $x^n - 1$, e o grau de $g(x)$ determina a dimensão k do código $[n, k]$, sendo $k = n - \deg(g(x))$.

A síndrome de uma palavra recebida $r(x)$ é calculada utilizando o polinômio gerador $g(x)$. Formalmente, a síndrome é definida como o resto da divisão de $r(x)$ por $g(x)$, isto é,

$$s(x) = r(x) \pmod{g(x)}.$$

Se $r(x)$ é um múltiplo de $g(x)$, então $r(x)$ é uma palavra-código válida. Caso contrário, a síndrome fornece informações sobre a posição e o valor do erro, permitindo a correção do erro.

Vamos apresentar como construir um código cíclico utilizando resíduos quadráticos. Para isso, seguimos as seguintes etapas:

1. Escolha de um número primo p .
2. Calcule os resíduos quadráticos $x^2 \pmod{p}$ para $x \in \{1, 2, \dots, p-1\}$.
3. Utilize os resíduos quadráticos para definir um polinômio gerador.

Exemplo 5.7. Neste exemplo, vamos considerar o corpo finito $\mathbb{F}_{11} = \{0, 1, 2, \dots, 10\}$. Vamos calcular os resíduos quadráticos e utilizá-los para construir o polinômio gerador de um código cíclico.

Primeiramente, determinamos os resíduos quadráticos em $\mathbb{F}_{11}$, isto é, os elementos que podem ser expressos como quadrados de outros elementos no corpo. Para cada elemento $x \in \mathbb{F}_{11}$, calculamos $x^2 \pmod{11}$:

$$\begin{aligned} 1^2 &\equiv 1 \pmod{11}, \\ 2^2 &\equiv 4 \pmod{11}, \\ 3^2 &\equiv 9 \pmod{11}, \\ 4^2 &\equiv 16 \equiv 5 \pmod{11}, \\ 5^2 &\equiv 25 \equiv 3 \pmod{11}, \\ 6^2 &\equiv 36 \equiv 3 \pmod{11}, \\ 7^2 &\equiv 49 \equiv 5 \pmod{11}, \\ 8^2 &\equiv 64 \equiv 9 \pmod{11}, \\ 9^2 &\equiv 81 \equiv 4 \pmod{11}, \\ 10^2 &\equiv 100 \equiv 1 \pmod{11}. \end{aligned}$$

Observamos que os resíduos quadráticos distintos em $\mathbb{F}_{11}$ são $\{1, 3, 4, 5, 9\}$. Estes resíduos serão utilizados como raízes para construir o polinômio gerador $g(x)$ de um código cíclico. O polinômio gerador $g(x)$ é definido como o produto dos fatores lineares associados a cada resíduo quadrático:

$$g(x) = (x - 1)(x - 3)(x - 4)(x - 5)(x - 9).$$

Após simplificarmos, obtemos que o polinômio gerador final é:

$$g(x) = x^5 - 22x^4 + 176x^3 - 638x^2 + 1023x - 540, \text{ isto é, } g(x) = x^5 - 10 \text{ em } \mathbb{F}_{11}.$$

5.3.2 Exemplo usando Sagemath

Nesta seção apresentamos o Exemplo 5.7 implementado no software Sagemath.

```

1
2 def construir_codigo_ciclico(p):
3     """
4     Constrói um código cíclico a partir dos resíduos quadráticos no
5     corpo finito F_p.
6     Entrada:
7         p - número primo
8     Saída:
9         - Lista de resíduos quadráticos
10        - Polinômio gerador g(x)
11        - Ordem do código cíclico
12    """
13
14    # Anel de polinômios sobre GF(p)
15    R.<x> = PolynomialRing(GF(p))
16
```

```

17     # Calcular os resíduos quadráticos mod p
18     quadratic_residues = sorted(set([(x^2) % p for x in range(1, p)]))
19     print(f"Resíduos quadráticos módulo {p}: {quadratic_residues}")
20
21     # Construir o polinômio gerador usando os resíduos quadráticos
22     g = prod([(x - r) for r in quadratic_residues])
23     print(f"Polinômio gerador: {g}")
24
25     # Determinar a ordem do código cíclico
26     n = p - 1 # 0 tamanho do corpo menos 1 (elementos não nulos)
27     k = n - g.degree() # Dimensão do código
28     print(f"Código cíclico [n, k]: [{n}, {k}]")
29
30     return quadratic_residues, g, (n, k)
31
32     # Exemplo de execução para um número primo p = 11
33     construir_codigo_ciclico(11)

```

Executando o código acima no SageMath, obtemos a seguinte resposta:

```

Resíduos quadráticos módulo 11: [1, 3, 4, 5, 9]
Polinômio gerador: x^5 + 10
Código cíclico [n, k]: [10, 5]
[24]: ([1, 3, 4, 5, 9], x^5 + 10, (10, 5))

```

[]:

Neste capítulo, exploramos algumas aplicações da Lei da Reciprocidade Quadrática, demonstrando sua importância e relevância em diversas áreas. Ao longo deste trabalho, evidenciamos como a Lei da Reciprocidade Quadrática não apenas resolve questões teóricas, mas também oferece ferramentas poderosas para a resolução de problemas práticos.

6 Considerações Finais

Neste trabalho foram apresentados conceitos fundamentais da teoria dos números, com ênfase nas congruências lineares, resíduos quadráticos e na Lei da Reciprocidade Quadrática. Inicialmente, revisamos as propriedades essenciais das congruências lineares, incluindo o Teorema Chinês do Resto, que tem papel central em várias áreas da matemática aplicada e computacional. Em seguida, discutimos os resíduos quadráticos, culminando no desenvolvimento do símbolo de Legendre e nas várias provas da Lei da Reciprocidade Quadrática.

Ao explorar as diversas provas da Lei da Reciprocidade Quadrática, destacamos três abordagens distintas, cada uma oferecendo diferentes perspectivas teóricas e aplicações. A primeira abordagem utilizou o lema de Eisenstein, fornecendo uma demonstração puramente aritmética. Já a segunda prova explorou o uso de raízes da unidade, conectando a reciprocidade quadrática a métodos da teoria dos números algébricos. A terceira prova, baseada na teoria dos grupos, estabeleceu uma ponte entre os conceitos de simetria e reciprocidade, oferecendo um ponto de vista algébrico para o problema.

No último capítulo, abordamos as aplicações práticas desses conceitos, com foco especial na criptografia. Discutimos o Sistema Criptográfico de Rabin, tanto na sua formulação original quanto na implementação no software SageMath, destacando o uso de congruências quadráticas como base para a segurança computacional. Além disso, exploramos o teste de primalidade de Solovay-Strassen, que também se baseia em resultados relacionados à reciprocidade quadrática.

Finalmente, analisamos aplicações mais avançadas da Lei da Reciprocidade Quadrática, como sua utilização em teoria dos grafos e na construção de códigos cíclicos.

Este trabalho mostra como conceitos aparentemente abstratos da aritmética podem encontrar aplicações diretas em problemas práticos, reforçando a importância da teoria dos números na matemática aplicada.

Esperamos que estudantes e professores possam fazer uso deste trabalho para o ensino e aprendizado dos temas abordados aqui e, dessa forma, difundir o conhecimento adquirido, e que este trabalho possa servir como base para aprofundamento teórico e prático, inclusive para sua utilização em sistemas computacionais.

Referências

- [1] LEMMERMEYER, F. *Reciprocity Laws: From Euler to Eisenstein*. [S.l.]: Springer Science & Business Media, 2000.
- [2] RABIN, M. O. Probabilistic algorithms for testing primality and factoring. *Journal of Number Theory*, v. 12, n. 1, p. 128–138, 1980.
- [3] SOLOVAY, R.; STRASSEN, V. A fast monte-carlo test for primality. *SIAM Journal on Computing*, v. 6, n. 1, p. 84–85, 1977.
- [4] MILLER, G. L. Riemann’s hypothesis and tests for primality. *Journal of Computer and System Sciences*, v. 13, n. 3, p. 300–317, 1976.
- [5] WEST, D. B. *Introduction to Graph Theory*. 2nd edition. ed. [S.l.]: Prentice Hall, 2001. ISBN 978-0130144003.
- [6] ZIMMERMANN, P. et al. *Calcul Mathématique avec Sage*. SageMath, 2020. Disponível em: <<http://dl.lateralis.org/public/sagebook/sagebook-ba6596d.pdf>>.
- [7] DEVELOPERS, T. S. Sage: Open source mathematical software. 2023. Versão 10.1. Disponível em: <<https://www.sagemath.org>>.
- [8] ROUSSEAU, S. *Quadratic and Cubic Reciprocity*. Dissertação (Master’s Thesis) — Eastern Washington University, 2012. EWU Masters Thesis Collection, 27. Disponível em: <<https://dc.ewu.edu/theses/27>>.
- [9] MATEMÁTICA, S. B. de. *Aritmética: Coleção do PROFMAT*. Rio de Janeiro, Brasil: Sociedade Brasileira de Matemática, 2019. ISBN 978-85-8453-008-4.
- [10] LANDAU, E. *Teoria Elementar dos Números*. Rio de Janeiro: Ed. Ciência Moderna, 2002.
- [11] VILLELA, A. H. e M. L. T. *Polinômios e Equações Algébricas*. 1. ed. Rio de Janeiro: Editora SBM, 2012.
- [12] SANTOS, J. P. *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 2012.

-
- [13] ALMUTERI, A. N. *Quadratic Reciprocity: Proofs and Applications*. Dissertação (Electronic Thesis) — University of Mississippi, 2019. Electronic Theses and Dissertations, 1540. Disponível em: <<https://egrove.olemiss.edu/etd/1540>>.
- [14] LEQUAIN, A. G. e Y. A. E. *Elementos de Álgebra*. 7. ed. Rio de Janeiro: Editora IMPA, 2022.
- [15] LEGENDRE, A. M. *Essai sur la theorie des nombres*. [S.l.]: Chez Courcier, imprimeur-libraire pour les mathematiques, 1808.
- [16] TAMAOKI, A. M. *Lei da Reciprocidade Quadrática*. [S.l.: s.n.], 2021.
- [17] IRELAND, K.; ROSEN, M. *A Classical Introduction to Modern Number Theory*. [S.l.]: Springer Science & Business Media, 2013. v. 84.
- [18] DUDLEY, U. *Elementary Number Theory*. [S.l.]: Courier Corporation, 2012.
- [19] ROUSSEAU, G. On the quadratic reciprocity law. *Journal of the Australian Mathematical Society*, v. 51, n. 3, p. 423–425, 1991.
- [20] LIMA, F. M.; SOUZA, M. F. *Códigos Corretores de Erros: Teoria e Aplicações*. Campinas: Editora UNICAMP, 2009. ISBN 978-85-268-0868-4.
- [21] GROSS, J. L.; YELLEN, J. *Teoria dos Grafos e suas Aplicações*. 2ª edição. ed. Porto Alegre: Bookman, 2012. ISBN 978-85-363-3154-4.
- [22] STINSON, D. R. *Introdução à Criptografia com Teoria de Chaves*. 2ª edição. ed. Porto Alegre: Bookman, 2003. ISBN 978-85-363-0308-4.
- [23] PLESS, V. *Introduction to the Theory of Error-Correcting Codes*. 3rd edition. ed. [S.l.]: John Wiley & Sons, 1989. ISBN 978-0471857872.
- [24] RABIN, M. O. *How to Exchange Secrets with Oblivious Transfer*. [S.l.], 1981. Disponível em: <https://eprint.iacr.org/2005/187.pdf>.

A Guia de Instalação do Software *SageMath* no Windows 10 e 11

O *SageMath* [6, 7], também conhecido como Sage, é um software matemático de código aberto amplamente utilizado para cálculos simbólicos, numéricos e algébricos, além de aplicações em diversas áreas da matemática e ciência computacional. Desenvolvido com o objetivo de integrar ferramentas avançadas em uma única plataforma, o *SageMath* combina bibliotecas renomadas como NumPy, SciPy, matplotlib, GAP, FLINT, entre outras, proporcionando um ambiente robusto e versátil para pesquisadores, professores e estudantes.

Uma das principais características do *SageMath* é sua flexibilidade, permitindo a realização de cálculos em álgebra abstrata, geometria algébrica, teoria dos números, análise matemática e estatística. Sua interface, baseada no Jupyter Notebook, facilita a interação com o software, oferecendo um ambiente dinâmico e intuitivo para o desenvolvimento de projetos matemáticos e científicos. Além disso, por ser um software de código aberto, o *SageMath* permite que a comunidade acadêmica contribua ativamente para sua evolução, garantindo sua atualização contínua e adequação às necessidades contemporâneas.

Atualmente, a versão 10.5 é a mais recente do *SageMath* disponível para download. As versões anteriores não estão mais acessíveis no site oficial.

<https://www.sagemath.org/>.

Abaixo estão as instruções detalhadas para instalação no sistema operacional Windows, utilizando o *Subsistema Windows para Linux* (WSL).

A versão utilizada do Ubuntu é a 22.04 LTS, pois possui em seu repositório a versão 9.5 do *SageMath*, usando versões mais recentes do Ubuntu é necessário compilar o *SageMath* da fonte, as instruções estão no link: https://sagemanifolds.obspm.fr/install_ubuntu.html

1. Acesse o link oficial: <https://doc.sagemath.org/html/en/installation/index.html>. O site apresenta instruções para instalação no Windows, MacOS e Linux. Este guia foca no procedimento para o sistema Windows.
2. No menu Iniciar do Windows, pesquise por **Ativar ou Desativar recursos do Windows**.
3. Ative os recursos **Plataforma do Hipervisor do Windows** e **Subsistema do Windows para Linux**, depois clique em "OK".

4. Reinicie o computador.
5. Abra a **Microsoft Store**, procure pela versão 22.04 LTS do **Ubuntu** e instale o programa.
6. Após a instalação, o Ubuntu solicitará a criação de um nome de usuário e senha.
 - Escolha um nome de usuário sem espaços.
 - Por questões de segurança, a senha não será exibida durante a digitação.
 - Guarde essa senha, pois ela será necessária para acessar o sistema Linux e obter privilégios de administrador para instalar ou modificar programas no Ubuntu.
7. No terminal do Ubuntu, execute os comandos abaixo, na sequência, para preparar o ambiente:

(a) **Atualizar os repositórios:**

```
sudo apt-get update
```

Digite a senha criada no passo anterior para confirmar.

(b) **Atualizar os pacotes do sistema:**

```
sudo apt-get upgrade
```

Pressione **Y** quando solicitado para confirmar a atualização.

(c) **Instalar o SageMath:**

```
sudo apt-get install sagemath
```

Novamente, pressione **Y** para confirmar. Este processo pode levar algum tempo, dependendo da velocidade de sua conexão com a internet.

8. Feche a janela do Ubuntu.
9. Abra o Ubuntu novamente e configure o ambiente para executar o *SageMath*:

(a) **Criar um novo ambiente Conda para o SageMath:**

```
conda create -n sage python=3.11
```

Pressione **Enter** para confirmar.

(b) **Ativar o ambiente criado:**

```
conda activate sage
```

(c) **Executar o SageMath com Jupyter Notebook:**

```
sage -n jupyter
```

10. Após executar o comando acima, será exibido um link no terminal, similar ao seguinte exemplo:

```
http://localhost:8888/tree?token=21b60ec20d37286dacdab32a5
```

Copie e cole o link no navegador para acessar o ambiente Jupyter Notebook com suporte ao *SageMath*.

11. **Utilizando o SageMath após a instalação:** Sempre que precisar utilizar o *SageMath*, siga os passos abaixo:

(a) Abra o Ubuntu.

(b) Ative o ambiente *SageMath* com o comando:

```
conda activate sage
```

(c) Execute o *SageMath* com o comando:

```
sage -n jupyter
```

(d) Copie e cole o link que será exibido na tela no navegador, semelhante ao exemplo:

```
http://localhost:8888/tree?token=21b60ec20d37286dacdab32a5
```