Instituto Federal de Educação, Ciência e
Tecnologia da Bahia - Campus Valença
Licenciatura em Matemática

Fabiane dos Santos Batista

Congruências: Resíduos Quadráticos e Representação de Inteiros como Soma de Quadrados

Valença-BA
2022

Fabiane dos Santos Batista

Congruências: Resíduos Quadráticos e Representação de Inteiros como Soma de Quadrados

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Educação, Ciência e Tecnologia da Bahia - *Campus* Valença como parte dos requisitos para a obtenção do título de Licenciada em Matemática.

Orientador: Prof. Dr. Diogo Soares Dórea da Silva

Valença-BA
2022

Fabiane dos Santos Batista

Congruências: Resíduos Quadráticos e Representação de Inteiros com Soma de Quadrados

Monografia apresentada a Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia da Bahia, *Campus* Valença, como requisito parcial para obtenção do título de Licenciada em Matemática.

Monografia aprovada em___/___/___.

BANCA EXAMINADORA

_____

Prof. Dr. Diogo Soares Dórea da Silva

Instituto Federal de Educação, Ciência e Tecnologia da Bahia

_____

Profa. Me. Ana Carolina Moura Teixeira

Instituto Federal de Educação, Ciência e Tecnologia da Bahia

_____

Prof. Me. Diego Coutinho Vieira Santiago

Instituto Federal de Educação, Ciência e Tecnologia da Bahia

Valença - BA,____de____de 2022.

B333c Batista, Fabiane dos Santos
Congruências: resíduos quadráticos e representação de inteiros como soma de quadrados/ Fabiane dos Santos Batista. - Valença - BA: IFBA, 2022.
41f.;il.

Orientador: Prof. Dr. Diogo Soares Dórea da Silva

Trabalho de conclusão de curso (Graduação) - Instituto Federal de Educação, Ciência e Tecnologia da Bahia – Campus Valença, 2022.

1.Teoria dos Números. 2.Congruências. 3. Resíduos Quadráticos. 4. Representação de inteiros como soma de quadrados. I. Silva, Diogo Soares Dórea da. II. Título.
CDD: 512

Ficha Catalográfica elaborada pela bibliotecária do IFBA campus Valença/ Cátia Almeida de Andrade CRB1403-5

Dedicatória

Eu dedico este trabalho à minha irmã Fernanda e também às minhas primas, Amanda, Bianca, Bruna, Isadora, Lara e Lorena, minhas preciosidades. Elas merecem um mundo onde as mulheres possam ocupar todos os espaços que quiserem, se isso fizer sentido para suas respectivas histórias. Precisam ter coragem para enfrentar seus medos e para conquistar seus lugares, onde quer que sejam.

Agradecimentos

Agradeço a Deus, meu Senhor, pelo dom da vida e por ser a minha esperança, força e motivação todos os dias, sem exceção.

Agradeço a Edna, minha mãe, um exemplo de força e perseverança para mim desde que me entendo por gente.

Agradeço a Fábio, meu pai, e Felipe, meu irmão, por me ensinarem a sonhar.

Agradeço a Emanuel, meu primo e melhor amigo, por me ouvir, impulsionar e acreditar em mim mesmo quando eu não fui capaz de fazer isso.

Agradeço a Isaack, meu namorado, por me fazer sentir especial, amada e capaz todos os dias.

Agradeço à minha família, amigos e colegas de trabalho por participarem da minha vida e me desejarem o melhor.

Agradeço a todos os docentes que contribuíram para minha formação acadêmica. Em especial:

- Ao estimado professor Diogo Soares Dórea da Silva (orientador), por ter me convidado para realizar este incrível trabalho, pela paciência, parceria e compreensão, por me dar suporte, treino e ter acreditado em mim;
- Aos queridos professores Roque da Silva Lyrio, Márcia Rebeca de Oliveira e Diego Coutinho Vieira Santiago, por terem um olhar sensível nos momentos que precisei;
- Às digníssimas professoras, Eliete da Silva Barros e Ruth da Silva Araújo, por tanto terem me ensinado através de longas discussões teóricas;
- Aos professores Diego Coutinho Vieira Santiago e Ana Carolina Moura Teixeira, por terem aceitado o convite para compor a banca e realizar valiosas contribuições.

Agradeço a todos os meus ex-alunos. Vocês, certamente, contribuíram para minha formação docente.

A Matemática Pura é, à sua maneira,
a poesia das ideias lógicas.

Albert Einstein (1879-1955)

Resumo

A Teoria dos Números é uma das grandes áreas da Matemática e o foco dos estudos nesta área é o comportamento dos números (principalmente inteiros) em condições específicas. Algumas relações podem ser feitas entre esses números ou estruturas que são estudadas, como a relação de divisibilidade. Esta relação foi explorada por muitos matemáticos e seu avanço resultou nas congruências. As congruências, especialmente, as congruências módulo m, com $m > 0$ e inteiro (que são exploradas nesta pesquisa), trazem muitos resultados interessantes como o conceito de resíduo. Sabe-se que toda a divisão deixa um resíduo, e não é diferente com um número elevado ao quadrado, que deixam os chamados Resíduos Quadráticos. E foi através desta importante definição, aliada à definição de Símbolo de Legendre, que foi possível compreender como se dá a Representação de Inteiros como Soma de Quadrados. Em virtude destes aspectos mencionados, o presente trabalho consiste numa revisão bibliográfica que tem o objetivo de estudar este tema. Para tanto, foram analisadas as obras: Hefez (2016), Burton (2016), Santos (2009), Merzbach (2012) e O'Regan (2016), que apresentam uma boa organização partindo das Congruências até a Representação de Inteiros como Soma de Quadrados. A conclusão do trabalho é de que todo número natural pode ser expresso como a soma de no máximo 4 quadrados (afirmação demonstrada pelo matemático Lagrange), e para alcançar este resultado, foram utilizadas ferramentas importantes como o Pequeno Teorema de Fermat, o Teorema de Euler e o Teorema de Wilson, além de vários outros resultados prévios apresentados, sobretudo em Congruências e Resíduos Quadráticos. Por fim, no Apêndice, apresentamos uma tabela com a "menor representação" como soma de quadrados para os 100 primeiros naturais e incluímos um teorema enunciado e provado pelo matemático Legendre que fala sobre os números que só podem ser expressos como a soma de quatro quadrados.

Palavras-chave: Teoria dos Números. Congruências. Resíduos Quadráticos. Representação de Inteiros como Soma de Quadrados.

Abstract

Number Theory is one of the major areas of mathematics and the focus of studies in this area is the behavior of numbers (mainly integer) under specific conditions. Some relationships can be made between these numbers or structures that are studied, such as the divisibility. This relationship was explored by many mathematicians and its advancement resulted in congruences. The congruences, especially the congruences module m, with $m > 0$ and integer (which are explored in this research), bring many interesting results such as the concept of residue. It is known that the any division leaves a residue, and is no different with a number squared, which leave the so-called Quadratic Residues. And it was through this important definition, combined with the definition of Legendre Symbol, that it was possible to understand how the Representation of Integers as Sum of Squares takes place. Due to these mentioned aspects, the present work consists of a bibliographic review that aims to study this theme. To this end, the works were analyzed: Hefez (2016), Burton (2016), Santos (2009), Merzbach (2012) and O'Regan (2016), which present a good organization from the Congruences to the Representation of Integers as the Sum of Squares. The conclusion of the work is that every natural number can be expressed as the sum of a maximum of 4 squares (result proved by the mathematician Lagrange), and to achieve this result, important tools such as Fermat's Little Theorem, Euler's Theorem and Wilson's Theorem were used, in addition to several other previous results presented, especially in Congruences and Quadratic Residues. Finally, in the Appendix, we present a table with the "smallest representation" as the sum of squares for the first 100 naturals and we included a theorem enunciated and demonstrated by the mathematician Legendre that talks about numbers that can only be expressed as the sum of four squares.

Keywords: Number Theory. Congruences. Quadratic Residues. Representing Integers as Sum of Squares.

Sumário

0 Motivação **1**

1 Introdução **2**

2 Congruências **4**

2.1 Uma Breve História das Congruências 4

2.2 Divisibilidade 7

2.2.1 Máximo Divisor Comum 12

2.3 Aritmética Modular 13

2.3.1 Resíduos 16

3 Ferramentas **18**

3.1 Numeros Primos 18

3.2 Pequeno Teorema de Fermat 19

3.3 Teorema de Euler 20

3.4 Teorema de Wilson 22

4 Resíduos Quadráticos **24**

4.1 Resíduos Quadráticos 24

4.2 Símbolo de Legendre e Critério de Euler 29

5 Representaçao de Inteiros como Soma de Quadrados **33**

5.1 O Problema de Waring 33

6 Conclusões e Perspectivas **37**

Referências **38**

A Representação dos 100 primeiros inteiros como soma de quadrados **39**

Capítulo 0

Motivação

Durante a minha trajetória acadêmica, eu sempre convivi com a Matemática de uma forma respeitosa. Frequentemente achava interessante as várias formas que ela poderia se apresentar e o fato de ser relacionada intimamente com as outras disciplinas.

Em algum momento, eu passei a ouvir das pessoas (especialmente dos meus professores) que eu iria acabar adentrando esta área. Isto mexeu comigo de alguma maneira, mas me mantive relutante para acreditar (até mesmo durante a Graduação).

Mesmo diante das dúvidas e dificuldades, eu resolvi cursar Licenciatura em Matemática e me envolvi, fui querendo conhecer melhor esta área pela qual já tinha tamanho apreço. Neste período, fui desenvolvendo uma série de trabalhos voltados para Educação, com o foco na Licenciatura, mas algo parecia estar faltando. Até então, eu achava que faria o TCC voltado para a área da Educação, mas quando me deparei com a disciplina "Estruturas Algébricas", alguma coisa mudou. Eu me divertia respondendo, tentando ou até mesmo errando. Portanto, quando o professor da disciplina, Diogo, me convidou para escrever este trabalho tudo fez sentido na hora, não houve hesitação, era isso o que faltava.

A minha motivação para escrever este trabalho é a de me divertir, aprender e valorizar esta área que eu tanto admiro. Eu não acredito que eu tenha o "perfil de alguém da Matemática Pura", mas desenvolver este trabalho, sem sombra de dúvidas, está sendo muito importante para a minha formação.

Espero que quem esteja lendo isso se sinta motivado para escrever (mesmo que também não se considere alguém com o perfil da área de Matemática Pura, você pode se surpreender) e não desista por causa das adversidades, pois elas estão presentes em todas as áreas.

Capítulo 1

Introdução

A Teoria dos Números estuda as mais variadas características dos números, como sua história, construção, representação, dentre outros aspectos. É uma área muito abrangente, mas este trabalho, em específico, tem interesse na Aritmética Modular (ou Congruências Módulo m, com $m \in \mathbb{N}$). Em virtude disto, tivemos que estudar divisibilidade, levando em conta suas propriedades e nuances, já que as congruências módulo m se baseiam firmemente em seus resultados.

Os resultados acerca das congruências foram pensados e elaborados por muitos matemáticos, sendo que o matemático com maior contribuição foi Gauss. Estes resultados partem dos resíduos até a representação de inteiros como soma de quadrados, conforme é descrito a seguir.

A presente pesquisa contém 4 capítulos de conteúdo essencialmente matemático, começando a contagem a partir do segundo capítulo. O Capítulo 2 traz alguns aspectos históricos das congruências, a sua definição e suas principais propriedades e resultados. Este é o maior capítulo desta pesquisa, porque ele será a base dos estudos posteriores, e é preciso apresentar toda essa parte básica para facilitar a compreensão destes capítulos seguintes, bem como para possibilitar a realização de demonstrações. Para tanto, tratamos acerca da divisibilidade e algumas definições que decorrem deste tópico.

O Capítulo 3 inicia tecendo alguns comentários a respeito dos números primos, como seus aspectos históricos e teoremas importantes, como o Teorema Fundamental da Aritmética. Ademais, são apresentadas três ferramentas essenciais para o desenvolvimento deste trabalho, são elas: o Pequeno Teorema de Fermat, o Teorema de Euler e o Teorema de Wilson. São ferramentas que possuem relação direta entre si e são fundamentais para a demonstração de teoremas específicos abordados no capítulo posterior.

O Capítulo 4 trata acerca dos resíduos quadráticos. É o capítulo que traz o aprofundamento do que é visto nos Capítulos 2 e 3 e é responsável por fazer a ligação destes capítulos com o Capítulo 5. Em outras palavras, os resíduos quadráticos surgem como resultados das congruências, se utilizam das ferramentas do Capítulo 3 para as demonstra-

ções dos seus teoremas e é o capítulo que vai possibilitar as provas dos teoremas do último capítulo. De fato, cabe destacar a importância do Símbolo de Legendre e do Critério de Euler, ambos apresentados neste referido capítulo, no desfecho do trabalho.

O quinto e último capítulo do presente trabalho inicia apresentando o Problema de Waring, que consiste em estudar a representação de naturais como soma de potências. Além disso, utilizamos os resultados construídos ao longo dessa pesquisa, a fim de enunciar e demonstrar o resultado principal deste estudo: o Teorema de Lagrange, que afirma que todo número natural pode ser escrito como uma soma de, no máximo, 4 quadrados.

Por fim, apresentamos no Apêndice, uma tabela autoral com a "menor representação" dos cem primeiros naturais como soma de quadrados. Ademais, enunciamos um teorema do matemático francês Legendre, que nos indica quais números só podem ser escritos como uma soma de quatro quadrados.

O presente trabalho trata-se de uma revisão bibliográfica e as referências utilizadas para a sua elaboração, foram: Hefez (2016), Burton (2016), Santos (2009), Merzbach (2012) e O'Regan (2016).

Capítulo 2

Congruências

Neste capítulo estudaremos alguns aspectos introdutórios e históricos das congruências, suas definições, resultados e aplicações no cotidiano, pois o que aqui for apresentado servirá como base para a construção dos capítulos posteriores. O capítulo foi dividido em 3 seções: Uma Breve História das Congruências, Divisibilidade e Aritmética Modular.

2.1 Uma Breve História das Congruências

Acredita-se que os estudos acerca de Teoria dos Números foram iniciados pelos egípcios e babilônios, mas esta área foi desenvolvida como uma teoria mais firme por Pitágoras (580-500 a.C., aproximadamente) e pelos membros da sua escola, conhecidos como pitagóricos. Eles estabeleceram muitas conexões entre os números e conceitos do cotidiano, tudo isso porque a finalidade dos envolvidos era contribuir para o desenvolvimento de argumentos filosóficos.

A Matemática começou a ser pensada para crescimento próprio, de fato, com a Escola de Alexandria, que foi destruída quando a cidade de Alexandria foi subjulgada pelos árabes em 641 a.C.. Após essa situação, foi construído um museu para guardar todos os conhecimentos possíveis que estavam sendo desenvolvidos em Alexandria. E, um dos maiores nomes ligados a esse museu, é o de Euclides (350-283 a.C.), que é conhecido atualmente por sua admirável contribuição na área da Geometria. Ademais, ele também foi o responsável por organizar todo conhecimento matemático desenvolvido até então e disponibilizá-lo para toda a sociedade no seu trabalho *Os Elementos*, o que inclui, por tabela, o que era conhecido sobre Teoria dos Números.

A Teoria dos Números é uma área de grande relevância para a Matemática. Essa área apresenta o comportamento dos números (especialmente inteiros) diante de situações previamente estabelecidas. E, de fato, aprofundando o estudo neste tão importante ramo, encontramos aplicações fundamentais para o desenvolvimento da sociedade tecnológica, como a Criptografia, bem como problemas não resolvidos, como a Conjectura de

Goldbach.

A Criptografia consiste em desenvolver e aplicar métodos de codificação de mensagens de tal forma que apenas os destinatários possam decodificar para ter conhecimento do seu conteúdo. Além disso, é uma área que se desenvolveu muito com o apoio da linguagem, posteriormente com o surgimento e aprimoramento dos computadores e atualmente com o seu uso através da manipulação de números primos.

É possível afirmar seguramente que os números primos elevaram os níveis de Criptografia que conhecíamos, isto porque são números que possuem alta complexidade. O sistema de Criptografia que utiliza como base os números primos funciona da seguinte maneira: são selecionados dois números primos muito grandes e distintos p e q. Sendo $m = p \cdot q$, é notório que é muito difícil descobrir os valores de p e q, tendo apenas o valor de m, por ser extremamente demorado e difícil fatorar números primos grandes. Em outras palavras, é fácil realizar esta operação (visto que é uma simples multiplicação), mas bastante difícil desfazer (decodificar), sendo uma tarefa relativamente mais simples apenas para o remetente que terá em sua posse a chave para a decodificação, ou seja, conhecimento do valor de p ou q.

Ainda não temos uma fórmula que forneça apenas números primos, mas temos números especiais e dentre eles, podemos destacar aqui os Números de Mersenne. Este nome foi dado em homenagem ao matemático e monge Marin Mersenne (1588-1648), que realizou estudos e interações com outros matemáticos que resultaram na fórmula $M_p = 2^p - 1$ com p primo, que é utilizada para gerar primos absurdamente grandes conhecidos como Primos de Mersenne. Um fato interessante, é que hoje, o maior número primo conhecido (e que é expresso através da fórmula de Mersenne) tem quase 25.000.000 de digitos.

Ademais, no que diz respeito aos números primos, o matemático nascido no Norte da Alemanha Cristian Goldbach (1690-1764) se debruçou sobre muitas ramificações matemáticas, e uma delas foi os números primos. Em um dos seus estudos, ele estabeleceu uma conjectura e enviou em formato de carta para Euler (1707-1783). Euler é considerado um dos maiores matemáticos que temos conhecimento atualmente e havia construído reputação internacional por contribuir em quase todos os ramos da Matemática Pura e Aplicada. Além disso, ele foi o responsável por desenvolver muitos estudos na época e estabelecer muitas notações que são utilizadas até hoje, como o e, que indica a base dos logaritmos naturais, muitas vezes chamado de "Número de Euler". Goldbach enviou esta carta lançando o palpite de que todo número inteiro par pode ser escrito como a soma de dois números que são ou primos ou 1. Uma formulação muito utilizada para descrever este palpite é o de que qualquer inteiro par maior que 4 pode ser escrito como a soma de dois números primos ímpares. E, de fato, é possível verificar esse palpite para os primeiros inteiros pares:

$$6 = 3 + 3$$
$$8 = 3 + 5$$
$$10 = 5 + 5$$

Euler respondeu a carta de Goldbach estabelecendo uma conjectura própria, que diz que qualquer número par maior que 6 na forma $2n+2$ é a soma de dois números sendo ou 1 ou primo na forma $4n+1$. Euler não comprovou a conjectura proposta por Goldbach, assim como nenhum outro matemático ao longo do tempo, mas é uma conjectura com base sólida, com fortes indícios de veracidade.

Mediante ao que foi apresentado por Goldbach e vários outros matemáticos, pode-se dizer que a Teoria dos Números potencializa o estudo sobre os números tentando categorizá-los, operá-los e relacioná-los de forma coerente. Isto, com o intuito de estabelecer definições que expressem a natureza comportamental dos números bem como ela é.

Diante de todas essas possibilidades, o já conhecido matemático Euclides desenvolveu um algoritmo capaz de revelar o maior divisor comum entre dois inteiros positivos. Ele notou, ao realizar sucessivas divisões com um olhar atento para os restos, que o último resto não-nulo é o maior divisor comum entre esses dois inteiros positivos dados. E com o passar do tempo, essa parte da Aritmética que envolve Divisibilidade foi sendo explorada e desenvolvida, abrindo espaço para a Aritmética Modular ou (como é comumente conhecida) *Congruência* módulo m (a todo momento durante este presente trabalho, sempre que for mencionado "*Congruência*", deve-se entender por "*Congruência* módulo m").

Utilizando corretamente o conceito de Congruência, é possível resolver problemas que seriam solucionados de forma muito trabalhosa, como por exemplo:

Qual o resto da divisão de 4^{555} por 7?

Este é um tipo de problema que assusta no primeiro momento, porque parece que para solucionar essa questão, é preciso desenvolver a potência, e em seguida, realizar a divisão por 7 a fim de obter o resto procurado. Mas a verdade é que por ser um problema focado no resto, pode ser resolvido facilmente por Aritmética Modular.

A maior parte do que é conhecido sobre Congruência nos dias atuais foi desenvolvida por Gauss (1777-1855). Aos 24 anos de idade, este brilhante e jovem matemático apresentou ao mundo os seus resultados acerca deste tópico fundamental da Teoria dos Números no seu trabalho *Disquisitiones Arithmeticae*, publicado em 1801. A sua influência é tão presente e os seus escritos tão respeitados que até hoje utilizamos a mesma notação proposta por ele na sua publicação.

Dito isto, para iniciarmos os estudos sobre as Congruências, primeiro estudaremos alguns tópicos da Divisibilidade na próxima seção deste capítulo, a fim de desenvolver uma boa base sobre as notações e resultados.

2.2 Divisibilidade

A Divisibilidade contém vários resultados e notações importantes que compõem a Aritmética Modular. Devido a isso, antes de iniciarmos os estudos que permeiam as Congruências, precisamos ter ciência do funcionamento da divisibilidade dos inteiros. Para iniciar, vamos nos ater à seguinte definição:

Definição 2.1. *Sejam dois inteiros a e b. Dizemos que a divide b se existir um inteiro c tal que $b = c \cdot a$.*

A notação para *a divide b* é $a \mid b$. Nós podemos dizer também, neste caso, que *a é um divisor ou fator de b*, ou que *b é múltiplo de a* ou até mesmo que *b é divisível por a.*

Exemplo 2.1. $1 \mid 6$, *pois* $6 = 1 \cdot 6$; $3 \mid 9$, *pois* $9 = 3 \cdot 3$; $5 \mid 0$, *pois* $0 = 5 \cdot 0$.

Algo importante a ser ressaltado acerca desta definição é que ela não define uma fração ou uma operação em $\mathbb{Z}$. Ela simplesmente define o que significa um inteiro a dividir outro inteiro b. E a negação desta sentença é que *a não divide b*, ou, $a \nmid b$, indicando que não existe um inteiro c que satisfaça a condição $b = c \cdot a$.

Exemplo 2.2. $3 \nmid 7$, *pois* $7 \neq 3k$; $8 \nmid 6$, *pois* $6 \neq 8p$; $4 \nmid 15$, *pois* $15 \neq 4q$, *para todos* $k, p, q \in \mathbb{Z}$.

Podemos, também, estabelecer algumas propriedades em decorrência da Definição 2.1, como veremos a seguir:

Proposição 2.1. *Dados $a, b, c \in \mathbb{Z}$, temos:*

(i) $1 \mid a$, $a \mid a$ e $a \mid 0$.

(ii) $0 \mid a \iff a = 0$.

(iii) $a \mid b$ se, e somente se, $|a| \mid |b|$.

(iv) se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração.

(i) a pode ser reescrito como $a = a \cdot 1$ o que implica que $1 \mid a$ e $a \mid a$. Além disso, já que $0 = a \cdot 0$, então $a \mid 0$, $\forall a \in \mathbb{Z}$.

(ii) Suponhamos que $0 \mid a$. Isto implica que existe um inteiro c, tal que $a = 0 \cdot c$. Disso, temos que $a = 0$ para todo e qualquer $c \in \mathbb{Z}$. Reciprocamente, como temos que $a = 0$, logo $a = 0 = 0 \cdot d$ para todo $d \in \mathbb{Z}$, portanto, $0 \mid a$.

(iii) Consideremos que $a \mid b$. Sendo assim, existe um $c \in \mathbb{Z}$, tal que, $b = c \cdot a$. Como os dois membros da equação possuem valores absolutos iguais, temos que $|b| = |c \cdot a|$. Dessa maneira, já que o produto dos módulos é igual ao módulo dos produtos, ficamos com $|b| = |c| \cdot |a|$, o que garante que $|a| \mid |b|$. Reciprocamente, vamos supor que $|a| \mid |b|$. Sendo assim, existe um $c \in \mathbb{Z}$ tal que $|b| = c \cdot |a|$. Acontece que para manter a igualdade, c precisa ser maior ou igual a 0. Portanto, podemos dizer que $c = |c|$. Substituindo esse resultado novo na equação que já tínhamos, ficamos com $|b| = |c| \cdot |a|$, e podemos escrever $|b| = |c \cdot a|$ devido ao fato do módulo do produto ser igual ao produto dos módulos. Assim, concluímos que $b = \pm(c \cdot a)$, implicando que $a \mid b$.

(iv) Como $a \mid b$ e $b \mid c$, temos que existem $d, e \in \mathbb{Z}$, tais que $b = ae$ e $c = bd$. Com esse resultado, se substituirmos o valor de b descrito na primeira equação na segunda, ficamos com $c = (ae)d$, e devido a associatividade da multiplicação, temos que $c = a(ed)$, o que nos indica que $a \mid c$.

□

Desses resultados, é possível retirar algumas informações importantes. Por exemplo, nas duas primeiras proposições chegamos à conclusão de que todo inteiro a é divisível por ± 1 e $\pm a$. Já vimos os casos positivos nas demonstrações acima, mas como a pode ser reescrito como $a = (-a) \cdot (-1)$, concluímos que tanto $-1 \mid a$, como $-a \mid a$ para todo a inteiro. Além disso, como $a \mid 0$ implica dizer que todo inteiro divide 0, logo, é correto dizer que o 0 tem infinitos divisores. Além disso, ao considerarmos que $a \mid 0$, se a for igual a 0, podemos concluir que $0 \mid 0$.

Agora, suponhamos que $a \mid b$, com $a \neq 0$. Seja c um inteiro tal que $b = c \cdot a$. Esse inteiro c é chamado, univocamente, de *quociente de b por a*, sendo representado por $c = \dfrac{b}{a}$. Vamos ver alguns exemplos que representam essas situações apresentadas:

Exemplo 2.3. $\dfrac{8}{1} = 8$; $\dfrac{8}{8} = 1$; $\dfrac{0}{-1} = 0$; $\dfrac{0}{2} = 0$; $\dfrac{9}{-3} = -3$.

Observação 2.1. *Perceba que* $\dfrac{b}{a}$ *só está definido quando* $a \neq 0$ *e* $a \mid b$.

Proposição 2.2. *Sejam* $a, b, c, d \in \mathbb{Z}$. *Se* $a \mid b$ *e* $c \mid d$, *então* $ac \mid bd$.

Demonstração. Se $a \mid b$ e $c \mid d$, então existem $e, f \in \mathbb{Z}$ tais que $b = ae$ e $d = cf$. Se multiplicarmos as duas equações, temos que: $bd = (ac)(ef)$, logo $ac \mid bd$. □

Exemplo 2.4. *Como* $2 \mid 4$ *e* $-3 \mid 9$, *então,* $(2 \cdot (-3)) \mid (4 \cdot 9)$, *ou seja,* $-6 \mid 36$.

Proposição 2.3. *Dados* $a, b, c \in \mathbb{Z}$, *se* $a \mid b$, *então* $ac \mid bc$.

Demonstração. Como $a \mid b$ e $c \mid c$ decorre, pela Proposição 2.2, que $ac \mid bc$. □

Exemplo 2.5. *Como temos que* $5 \mid 10$*, então,* $5 \cdot 3 \mid 10 \cdot 3$*, logo,* $15 \mid 30$*.*

Proposição 2.4. *Sejam* $a, b, c \in \mathbb{Z}$*. Se* $a \mid b$ *e* $a \mid c$*, então,* $a \mid (b \pm c)$*.*

Demonstração. Como $a \mid b$ e $a \mid c$, então $b = a \cdot q$ e $c = a \cdot p$, sendo $q, p \in \mathbb{Z}$. Somando estas equações, temos que $b + c = a \cdot q + a \cdot p$. Colocando, agora, a em evidência, ficamos com $b+c = a \cdot (q+p)$ e, portanto, $a \mid (b+c)$. Agora, se ao invés de somarmos, subtrairmos as equações, temos que $b - c = a \cdot q - a \cdot p$. Colocando a em evidência, novamente, nós ficamos com $b - c = a \cdot (q - p)$. Logo, $a \mid (b - c)$.

□

Exemplo 2.6. *Tendo em vista que* $4 \mid 8$ *e* $4 \mid 12$*, então* $4 \mid (8 - 12)$ *e* $4 \mid (8 + 12)$*, ou seja,* $4 \mid -4$ *e* $4 \mid 20$*, respectivamente.*

Proposição 2.5. *Se* $a, b, c \in \mathbb{Z}$ *são tais que* $a \mid b$ *e* $a \mid c$*, então, para todos* $x, y \in \mathbb{Z}$*, temos que* $a \mid (xb + yc)$*.*

Demonstração. Se $a \mid b$ e $a \mid c$, então existem f e g que pertencem a $\mathbb{Z}$, tais que: $b = fa$ e $c = ga$. Multiplicando a primeira equação por x, temos que $xb = x(fa)$ e multiplicando a segunda equação por y, ficamos com $yc = y(ga)$. Somando as duas equações, temos que $xb + yc = x(fa) + y(ga) = (xf + yg)a$, o que mostra que $a \mid (xb + yc)$.

□

Exemplo 2.7. *Como* $2 \mid 6$ *e* $2 \mid 4$*, então* $2 \mid (6 \cdot (-3) + 4 \cdot 5)$*. Dessa forma, temos que* $2 \mid (-18 + 20)$*, ou seja,* $2 \mid 2$*.*

Proposição 2.6 (Lema de Gauss)**.** *Dados* $a, b, c \in \mathbb{Z}$*, se* $a \mid bc$ *e* a *e* b *são primos entre si, então* $a \mid c$*.*

Demonstração. Pelo Teorema 2.1, existem x e y inteiros de tal forma que $xa + yb = 1$. Ao multiplicarmos os dois membros desta equação por c obtemos $x(ac) + y(bc) = c$. Como sabemos que $a \mid ac$, e por hipótese, temos que $a \mid bc$, então, pela Proposição 2.5, concluímos que $a \mid c$. □

Exemplo 2.8. $2 \mid 4 \cdot 7$*, e como* $(2, 7) = 1$*, temos que* $2 \mid 4$*.*

Proposição 2.7. *Dados* $a, b \in \mathbb{Z}$*, em que* $b \neq 0$*, temos que* $a \mid b \Rightarrow |a| \leq |b|$*.*

Demonstração. Consideremos que $a \mid b$. Se isso ocorre, então existe um $c \in \mathbb{Z}$ tal que $b = c \cdot a$. Como os dois membros da igualdade possuem valores absolutos equivalentes, temos que $|b| = |c \cdot a|$, e consequentemente, $|b| = |c| \cdot |a|$. Como já foi dito que $b \neq 0$, então, $c \neq 0$. O que decorre desta situação é que $|c| \geq 1$, nos fazendo concluir que $|a| \leq |c| \cdot |a| = |b|$, e, portanto, $|a| \leq |b|$.

□

Exemplo 2.9. *Como* $4 \mid -20$*, então,* $|4| \leq |-20|$*, ou seja,* $4 \leq 20$*.*

Temos algumas outras proposições que podem ser muito úteis para o estudo de divisibilidade.

Proposição 2.8. *Dados* $a, b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$*, temos que* $(a-b)$ *divide* $(a^n - b^n)$*.*

Demonstração. Essa prova será realizada por indução sobre n.

Base de Indução. Primeiro, para $n = 1$, temos que $(a-b) \mid (a^1 - b^1)$, o que é de fato verdade.

Hipótese de Indução. Vamos supor, agora, que $(a-b) \mid (a^n - b^n)$, e com isso, nos resta desenvolver $a^{n+1} - b^{n+1}$. Podemos reescrever $a^{n+1} - b^{n+1}$ como sendo $aa^n - bb^n$ e adicionar à essa expressão, $-ba^n + ba^n$. Dessa forma, ficamos com:

$$a^{n+1} - b^{n+1} = aa^n - ba^n + ba^n - bb^n.$$

Com isso, podemos colocar a^n e b em evidência, resultando em:

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

Assim, para melhor visualização, podemos organizar como:

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

Passo de Indução. Como é sabido que $(a-b) \mid (a^1 - b^1)$ que é a base de indução, e que por hipótese, $(a-b) \mid (a^n - b^n)$, podemos dizer, pela Proposição 2.5, que $(a-b) \mid (a^{n+1} - b^{n+1})$, para todo $n \in \mathbb{N}$.

□

Exemplo 2.10. $(5-2) \mid (5^2 - 2^2)$*, ou seja,* $3 \mid (25-4)$*, o que implica que* $3 \mid 21$*.*

Uma aplicação interessante que pode ser utilizada a partir disso, é que todo número escrito na forma $10^n - 1$, no qual $n \in \mathbb{N}$, é divisível por 9. Isso acontece porque $(a-b) \mid (a^n - b^n)$, logo, se fizermos $a = 10$ e $b = 1$, $a - b = 10 - 1 = 9$, então, $9 \mid 10^n - 1$.

Observação 2.2. *Uma outra maneira de checar este resultado, é percebendo que* $10^n - 1 = \underbrace{999\ldots9}_{n \text{ vezes}}$.

Proposição 2.9. *Sendo* $a, b \in \mathbb{Z}$*, temos que* $(a+b)$ *divide* $(a^{2n} - b^{2n})$*.*

Demonstração. Seguindo a mesma linha da prova anterior, vamos realizar a prova por indução.

Base de Indução. Vamos verificar, primeiramente, que a afirmação é válida para $n = 1$. Verficamos que é, de fato, verdade, pois $a+b$ divide $a^2 - b^2$, já que $a^2 - b^2$ pode ser reescrito como $(a+b) \cdot (a-b)$.

Hipótese de Indução. Para continuar, vamos supor que essa afirmação é válida para n, e vamos verificar se é válida para $n+1$. Se substituirmos n por $n+1$ na expressão $a^{2n} - b^{2n}$, teremos

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

Agora vamos adicionar os termos $-b^2a^{2n} + b^2a^{2n}$. E assim, ficamos com

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

Passo de Indução. Sabemos que $a+b$ divide $a^2 - b^2$, por ser a base de indução, e que, por hipótese, $a^{2n} - b^{2n}$ é divisível por $a+b$. Portanto, pela Proposição 2.5, temos a prova por concluída e válida para todo $n \in \mathbb{N}$.

□

Exemplo 2.11. *Temos que* $(5+7) \mid (5^{2\cdot2} - 7^{2\cdot2})$*, ou seja,* $12 \mid (625 - 2.401)$*, o que implica que* $12 \mid 1.776$.

Agora, veremos aspectos básicos da Divisão Euclidiana, que é um aprimoramento do estudo de Divisibilidade.

O princípio para o entendimento deste algoritmo é que, mesmo quando um inteiro $a \neq 0$ não divide um inteiro b de forma exata, ou seja, deixando resto 0, nós podemos realizar esta divisão e contabilizar o resto. Isso foi trazido de forma não-explícita, por Euclides, no seu trabalho *Os Elementos*. Vamos entender melhor o que foi dito, através dos exemplos abaixo:

Exemplo 2.12. *O quociente e o resto da divisão de 13 por 2 são* $q = 6$ *e* $r = 1$*, pois* $13 = 2 \cdot 6 + 1$*. Da mesma forma, o quociente e o resto da divisão de -17 por 5 são respectivamente* $q = -4$ *e* $r = 3$*, porque* $-17 = 5 \cdot (-4) + 3$.

Se o resto da divisão de um inteiro m por 2 for 0, temos que esse inteiro m é par e pode ser escrito na forma $m = 2n$, com $n \in \mathbb{N}$. Se o resto da divisão de um inteiro m por 2 for 1, temos que esse inteiro m é ímpar e pode ser escrito na forma $m = 2n + 1$, com $n \in \mathbb{N}$.

Se considerarmos um número natural m, tal que $m \geq 2$, podemos escrever qualquer número n de modo único na forma $mq + r$, sendo que $r, q \in \mathbb{Z}$ e $0 \leq r < m$.

Levando em conta as formas $3k, 3k+1, 3k+2$, com $k \in \mathbb{Z}$, todo inteiro m só se enquadrará em uma, e apenas uma, dessas formas apresentadas. Por exemplo, o número 13 pode ser representado como $3k + 1$, para $k = 4$, pois $3 \cdot 4 + 1 = 13$.

O mesmo acontece se considerarmos as formas $4k, 4k+1, 4k+2, 4k+3$, com $k \in \mathbb{Z}$. Um inteiro qualquer só poderá ser representado por uma dessas formas.

2.2.1 Máximo Divisor Comum

O Máximo Divisor Comum (mdc) tem uma importância notável para o que será estudado posteriormente no presente trabalho, que são os Resíduos Quadráticos e a Representação de Inteiros como Soma de Quadrados. Por isso, vamos apresentar nesta subseção alguns dos seus resultados e implicações mais importantes.

Definição 2.2. *Sendo $a, b, d \in \mathbb{Z}$, $d \geq 0$, d será chamado divisor comum de a e b se $d \mid a$ e $d \mid b$.*

Exemplo 2.13. *Os números $\pm 1, \pm 2, \pm 4$ são os divisores em comum de 16 e 20.*

Diante disso, Euclides apresenta no seu trabalho *Os Elementos*, o mdc, como sendo definido pelas propriedades abaixo:

Proposição 2.10. *Sejam $a, b, d \in \mathbb{Z}$, com $d \geq 0$. Então, d será considerado mdc de a e b, se:*

(i) d é divisor comum de a e de b;

(ii) se d é divisível por todos os divisores de a e de b.

Uma implicação importante se constrói devido a (ii). Se d e d' são mdc de um par de inteiros, então, $d \mid d'$ e $d' \mid d$. Somando isso ao fato de que o mdc é um inteiro positivo, temos que $d \geq 0$ e $d' \geq 0$. Isto implica que $d = d'$. Ou seja, o mdc é único.

A notação para o mdc de dois números inteiros a e b é (a, b). Ademais, não importa a ordem destes inteiros ao serem inclusos na notação, ou seja, $(a, b) = (b, a)$. Além disso, temos alguns casos em que é fácil verificar qual é o mdc, por exemplo:

(i) $(0, a) = |a|$;

(ii) $(1, a) = 1$;

(iii) $(a, a) = |a|$.

Levando estes resultados adiante, se $a \mid b$, então $(a, b) = |a|$, para todos $a, b \in \mathbb{Z}$. De fato, neste caso, o a é divisor de b e divisor dele mesmo, ou seja, a é *divisor comum* desse par de inteiros. Se existir outro divisor comum c de a e b, este c então divide a, mostrando que $|a|$ é o maior divisor comum entre esses dois números a e b. A recíproca é verdadeira, pois se $(a, b) = |a|$, então $|a| \Big| b$, e conclui-se que $a \mid b$.

Com relação a notação do mdc de dois números, é válido ressaltar que, sendo (a, b) com $a, b \in \mathbb{Z}$, então $(a, b) = (a, -b) = (-a, b) = (-a, -b)$. Devido a este resultado, normalmente são sempre utilizados valores não-negativos tanto para a quanto para b.

Ademais, pela Proposição 2.1, temos que todo número inteiro divide 0. Dessa forma, o mdc de a e b é 0 quando $a = b = 0$, pois 0 é o único que é divisível por todos os divisores

de 0. Da mesma maneira, temos que se $(a, b) = 0$, então $0 \mid a$ e $0 \mid b$. E como o único número divísivel por 0 é o próprio 0, concluímos que $a = b = 0$.

Apesar disso, o mdc de dois números inteiros não-nulos envolve mais alguns detalhes que requerem atenção. De fato, sendo um inteiro $d > 0$ um mdc entre dois inteiros a e b, tais que $a, b \neq 0$, e supondo que exista um *divisor comum* c qualquer desses dois valores, então $c \leq |c| \leq d$.

Normalmente, no Ensino Fundamental, se define mdc de dois inteiros $a, b \neq 0$ como sendo o maior número do conjunto dos *divisores comuns* desses dois números. Essa definição não está incorreta, mas não abrange os resultados de uma definição mais completa, como a que é apresentada na (ii) da Proposição 2.10.

Visto que já foi apresentada uma boa base do funcionamento do mdc, consideraremos o Teorema a seguir, que será necessário para demonstrar resultados posteriores.

Teorema 2.1 (Identidade de Bézout)**.** *Se d é o mdc de a e b, então existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = x_0 a + y_0 b$.*

Este Teorema não será provado, apenas tomaremos seu enunciado como verdadeiro. E uma coisa muito interessante sobre ele é a sua clara relação com a Proposição 2.5.

2.3 Aritmética Modular

Nesta seção traremos as noções iniciais de Congruências, suas especificidades e seus resultados mais importantes para o desenvolvimento deste presente trabalho.

Tem-se uma congruência entre dois valores $a, b \in \mathbb{Z}$ quando eles produzem o mesmo resto após serem realizadas as divisões euclidianas desses valores por um número natural m. Sintetizando este enunciado, chegamos na definição a seguir:

Definição 2.3. *Sejam $a, b, q, q' \in \mathbb{Z}$ e $m \in \mathbb{N}$. Considera-se que a é congruente a b módulo m, se existir um r tal que, $a = mq + r$ e $b = mq' + r$, com $0 \leq r < m$.*

Neste caso, dizemos que eles são côngruos ou congruentes, e denotamos $a \equiv b \bmod m$.

Exemplo 2.14. $11 \equiv 7$ *mod 2, pois tanto o 11 quanto o 7, quando divididos por 2, deixam resto 1 :* $11 = 2 \cdot 5 + 1$ *e* $7 = 2 \cdot 3 + 1$.

Considerando isso, temos que quando a e b deixam restos diferentes quando divididos por m, dizemos que a e b não são congruentes ou são incongruentes módulo m, ou seja, $a \not\equiv b \bmod m$.

Exemplo 2.15. $7 \not\equiv 6$ *mod* 3*, pois 7 dividido por 3 deixa resto 1 e 6 dividido por 3 deixa resto 0. Como* $0 \leq 0 \neq 1 < 3$*, tem-se que 7 e 6 são incongruentes quando divididos por 3.*

Teorema 2.2. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 0$. Consideramos $a \equiv b \mod m$ se, e somente se, $m \mid (b - a)$.*

Demonstração. Se $a \equiv b \mod m$, então, pela Definição 2.3, existem q, q' e r inteiros, com $0 \leq r < m$, tais que $a = qm + r$ e $b = q'm + r$. Logo, se subtrairmos a de b, temos que $b - a = (q' - q) \cdot m$, o que nos diz que $m \mid (b - a)$.

Reciprocamente, se $m \mid (b-a)$, então temos duas possibilidades, ou b e a são múltiplos de m, ou b e a deixam, respectivamente, restos r' e r não-nulos quando divididos por m. Para o primeiro caso, teremos $b = q'm$ e $a = qm$, o que faz com que ambos deixem resto 0 quanto divididos por m. Para o segundo caso, a e b deixam resto r e r', respectivamente, quando divididos por m. Assim, $b - a = (q' - q) \cdot m + (r' - r)$. Dessa forma, temos que $0 \leq |r' - r| < m$, e a única forma de m dividir $|r' - r|$ é quando $r' = r$, ou seja, $a \equiv b \mod m$. □

Uma aplicação muito interessante das congruências no cotidiano é o funcionamento do relógio. Ele é construído em um sistema de congruências módulo 12. Neste caso, se o relógio está marcando 5 horas e se passa uma volta completa, ou seja, 12 horas, vamos ter 17 horas, o que implica que $5 \equiv 17 \mod 12$.

Note que se for utilizado o módulo 1 para explorar as congruências de inteiros, não será possível obter bons resultados, pois quaisquer inteiros $a, b \in \mathbb{Z}$ são côngruos mod 1, visto que esses números inteiros quando divididos por 1 deixam resto 0. Devido a essa simplicidade que se impõe sobre as congruências mod 1, serão consideradas apenas as congruências mod m, com $m \in \mathbb{N}$ e $m > 1$, para obtenção de melhores resultados.

Proposição 2.11. *Sendo $a, b, m \in \mathbb{Z}$, com $m > 0$, consideramos que $a \equiv b \mod m$ se, e somente se, existir um $q \in \mathbb{Z}$ tal que $b = a + qm$.*

Demonstração. Considerando que $a \equiv b \mod m$, temos que $m \mid (b - a)$. Logo $b - a$ é um múltiplo de m e pode ser escrito como $b - a = qm$, o que mostra a existência de um inteiro q tal que $b = a + qm$. A recíproca conta com a existência de um q, tal que $b = a + qm$. Adicionando $-a$ aos dois membros dessa igualdade ficamos com $b - a = a - a + qm$ ou simplesmente $b - a = qm$. Isso nos diz que $b - a$ é múltiplo de m, implicando que $m \mid b - a$, e portanto, $a \equiv b \mod m$. □

Proposição 2.12. *Sejam $a, b, c \in \mathbb{Z}$ e $m \in \mathbb{N}$. Temos:*

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

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

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

Demonstração. Vamos aplicar o Teorema 2.2 para provar essas proposições.

(i) Como $m \mid 0$, podemos escrever esta afirmação como $m \mid (a-a)$, que nos indica, pelo Teorema 2.2, que $a \equiv a \bmod m$, $\forall\, a \in \mathbb{Z}$.

(ii) Supondo que $a \equiv b \bmod m$, podemos escrever $a = mq + r$ e $b = mq' + r$, com $q, q', r \in \mathbb{Z}$. E subtraindo a por b, temos que $a - b = m \cdot (q - q')$, o que mostra que $m \mid (a - b)$. Portanto, pelo Teorema 2.2, concluímos que $b \equiv a \bmod m$.

(iii) Se $a \equiv b \bmod m$, então $m \mid (b - a)$. E se $b \equiv c \bmod m$, então, $m \mid (c - b)$. Dessa forma, pela Proposição 2.4, $m \mid (b - a) + (c - b)$, ou seja, $m \mid (c - a)$, implicando que $a \equiv c \bmod m$.

□

Observação 2.3. *As proposições apresentadas anteriormente, com relação as congruências no conjunto dos inteiros, indicam que esta operação* ($\equiv$) *define uma relação de equivalência.*

Um dos resultados mais úteis e fortes que as Congruências apresentam é que elas são preservadas com relação a soma e a multiplicação. Vamos compreender melhor essa propriedade nas proposições a seguir.

Proposição 2.13. *Sejam $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{N}$ tal que $m > 1$. Temos:*

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

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

Demonstração. Como $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $m \mid (b - a)$ e $m \mid (d - c)$.

(i) Realizando a soma, nós temos que $m \mid (b-a)+(d-c)$. Logo, temos $m \mid (b+d)-(a+c)$. Portanto, concluímos que $(a + c) \equiv (b + d) \bmod m$.

(ii) Podemos escrever $b-a = qm$, com $q \in \mathbb{Z}$. Multiplicando os dois lados desta equação por d, temos que $bd - ad = dqm$, ou simplesmente, $d(b - a) = dqm$, que nos diz que $m \mid d(b - a)$. Da mesma forma, podemos escrever $d - c = q'm$, com $q' \in \mathbb{Z}$. Multiplicando os dois lados desta equação por a, temos que $ad - ac = aq'm$, ou simplesmente, $a(d - c) = aq'm$, que nos diz que $m \mid a(d - c)$. Pelo item anterior, podemos afirmar $m \mid d(b - a) + a(d - c)$, portanto, $m \mid (bd - ac)$.

□

Proposição 2.14. *Dados, $m, n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$, temos que se $a \equiv b \bmod m$, então $a^n \equiv b^n \bmod m$.*

Demonstração. A prova será realizada por indução sobre n.

Base de Indução. Primeiramente, vamos verificar se a afirmação é válida para $n = 1$. Nesse caso, temos que $a^1 \equiv b^1 \bmod m$. Portanto, concluímos que para $n = 1$ é válida.

Hipótese de Indução. Vamos assumir agora que a proposição é válida para algum n, ou seja, teremos que considerar que $a^n \equiv b^n \bmod m$.

Passo de Indução. Agora, verificaremos se a proposição é válida para $n+1$. Para isso, observe que $a^n \cdot a^1 \equiv b^n \cdot b^1 \bmod m$. Considerando a hipótese de indução e também a Proposição 2.13, segue que $a^{n+1} \equiv b^{n+1} \bmod m$.

□

Proposição 2.15. *Dados a, b, c, d e m inteiros, com $m > 0$, se $ac \equiv bc \bmod m$, então $a \equiv b \bmod m/d$, com $d = (c, m)$.*

Demonstração. Como $ac \equiv bc \bmod m$, temos que $bc - ac = qm$ para algum $q \in \mathbb{Z}$. Então $c \cdot (b - a) = qm$. Dividindo os dois membros da equação por d, ficamos com $c/d \cdot (b - a) = q \cdot m/d$. Ou seja, $m/d \mid c/d \cdot (b - a)$. Como $(m/d, c/d) = 1$, temos, pela Proposição 2.6, que $m/d \mid (b - a)$, o que implica que $a \equiv b \bmod (m/d)$. □

O teorema a seguir não será provado, mas seu resultado será aceito e utilizado para demonstrações futuras.

Teorema 2.3. *Dados $a, b, m \in \mathbb{Z}$, com $m > 0$ e $(a, m) = d$, se tivermos $ax \equiv b \bmod m$, caso $d \nmid b$, a congruência não tem solução e caso $d \mid b$, a congruência tem exatamente d soluções incongruentes módulo m.*

Agora que foram apresentadas as propriedades e definições mais importantes para o desenvolvimento do trabalho, podemos responder a questão que foi levantada no ínicio do capítulo, trazida no exemplo abaixo.

Exemplo 2.16. *Qual o resto da divisão de 4^{555} por 7?*

Resolução. Sabe-se que $4^3 = 64$ que dividido por 7 deixa resto 1, ou seja, $4^3 \equiv 1 \bmod 7$. De posse desta informação, temos que $4^{555} \equiv (4^3)^{185} \bmod 7$. Assim, podemos substituir o 4^3 por 1, ficando com $(4^3)^{185} \equiv 1^{185} \bmod 7$. E como $1^{185} \equiv 1 \bmod 7$, concluímos que o resto da divisão de 4^{555} por 7 é 1. □

2.3.1 Resíduos

Nesta subseção, abordaremos os resíduos de uma Congruência, perpassando as suas definições e implicações de forma breve. Para tanto, vamos nos ater ao que diz a definição a seguir.

Definição 2.4. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 0$. Se $b \equiv a \bmod m$, dizemos que a é um resíduo de $b \bmod m$.*

Com base nesta definição, podemos dizer que um Sistema Completo de Resíduos módulo m é um conjunto que contém todos os possíveis restos numa divisão de inteiros por m também inteiro. Dessa forma, os elementos pertencentes a este conjunto não podem ser repetidos, e isto é sintetizado por meio da definição a seguir.

Definição 2.5. *Tem-se que* $\{r_1, r_2, r_3, ..., r_i, ..., r_j\}$ *é um sistema completo de resíduos módulo* m *quando*

(i) $r_i \not\equiv r_j \bmod m$, para $i \neq j$;

(ii) Para todo $n \in \mathbb{Z}$, existe $r_i \mid n \equiv r_i \bmod m$.

Observação 2.4. *Um sistema completo de resíduos módulo* m *tem* m *elementos.*

Exemplo 2.17. $\{0, 1, 2, 3, \ldots, m-1\}$ *é um sistema completo de resíduos módulo* m.

Exemplo 2.18. $\{17, 4, -13, 18\}$ *é um sistema completo de resíduos mod* 4. *De fato,* $17 \equiv 1$ *mod* 4, $4 \equiv 0$ *mod* 4, $-13 \equiv 3$ *mod* 4 *e* $18 \equiv 2$ *mod* 4, *respectivamente.*

Da mesma forma que temos um *sistema completo de resíduos*, podemos ter um *sistema reduzido de resíduos* (SRR).

Definição 2.6. *Entende-se o conjunto* $\{r_1, r_2, r_3, ..., r_i, ..., r_j\}$ *por sistema reduzido de resíduos módulo* m, *se ele for um sistema completo de resíduos no qual foram retirados todos os valores* r_i *tais que* $(r_i, m) \neq 1$, *para* $i = 1, 2, 3, ..., s$, *com* $s \in \mathbb{N}$.

Exemplo 2.19. *{1,5} é um sistema reduzido módulo 6. De fato, um sistema completo neste caso seria {0,1,2,3,4,5}, e os únicos elementos que possuem o mdc igual a 1 quando formam par com o 6 são 1 e 5.*

Dessa maneira, temos não apenas esta subseção, mas o capítulo por concluído. Nele apresentamos as ferramentas e resultados mais necessários para o desenvolvimento desta pesquisa. Ademais, construímos uma boa base de conhecimento para o estudo da seção posterior, na qual iremos verificar alguns teoremas que seram utilizados como ferramentas nos próximos capítulos.

Capítulo 3

Ferramentas

Neste capítulo serão apresentados alguns enunciados sobre os números primos e três teoremas muito úteis para a formulação de resultados nos estudos dos Resíduos Quadráticos e, por sua vez, na Representação de Inteiros como Soma de Quadrados. Abordaremos o Pequeno Teorema de Fermat, o Teorema de Euler e o Teorema de Wilson, e para tanto, precisaremos definir, primeiramente, o que são números primos.

3.1 Numeros Primos

Definição 3.1. *Seja $p \in \mathbb{N}$, com $p > 1$. Dizemos que p é um número primo, se os únicos divisores naturais de p forem o 1 e o próprio p.*

Exemplo 3.1. *Podemos citar como exemplos de primos: 2,3,5,7,11,13,17,... . Eles são os primeiros números primos e são relativamente fáceis de se encontrar, simplesmente aplicando a definição, por serem "pequenos".*

Observação 3.1. *Os números que não se encaixam nessa definição de números primos, ou seja, apresentam mais divisores além do 1 e dele mesmo, são chamados números compostos, como por exemplo: 4,6,8,9,10,12,... .*

Os números primos e suas particularidades possibilitam o avanço da Matemática em diversas áreas. Como evidência disso, será apresentado, a seguir, o Teorema Fundamental da Aritmética, que não será demonstrado.

Teorema 3.1 (Teorema Fundamental da Artimética)**.** *Todo inteiro maior que 1 pode ser expresso como um produto de fatores primos, sendo essa fatoração única (e com ordem desprezada).*

Também existe um lema importante e útil sobre os primos que foi proposto por Euclides que cabe aqui ser destacado.

Lema 3.1 (Lema de Euclides)**.** *Dados $a, b, p \in \mathbb{Z}$, com p primo, se $p \mid ab$, então, $p \mid a$ ou $p \mid b$.*

Demonstração. Como $p \mid ab$ e p é primo, se tivermos que $p \nmid a$, então, pela Proposição 2.6, $p \mid b$. A situação seria análoga se $p \nmid b$, pois teríamos que $(b, p) = 1$, e pela Proposição supracitada, conhecida como Lema de Gauss, resultaria que $p \mid a$. □

3.2 Pequeno Teorema de Fermat

Desde a antiguidade, já era sabido que se p é primo, então $p \mid 2^p - 2$. A generalização desse resultado foi apresentada por Pierre de Fermat (1601-1665), através de um pequeno, porém bem elaborado teorema.

Fermat nasceu na França e realizou grandes descobertas no ramo da Matemática. Porém, diferentemente do que muitos pensam, ele não era matemático no sentido profissional da palavra e não mostrou interesse por isso até pelo menos os 30 anos. Na verdade, ele atuava como advogado e magistrado e, em algum momento, passou a se dedicar à Matemática nas horas vagas.

Pierre de Fermat, conhecido como "o príncipe dos amadores", ajudou a construir a Geometria Analítica e a formular bases técnicas para o Cálculo Diferencial e Integral e Probabilidade. Mas, a sua grande paixão era a abstração proposta pela Teoria dos Números. Dito isto, vamos verificar uma de suas grandes constribuições: o Pequeno Teorema de Fermat.

Teorema 3.2 (Pequeno Teorema de Fermat)**.** *Sejam $a, p \in \mathbb{N}$ tal que p é primo. Se $p \nmid a$, então, $a^{p-1} \equiv 1 \ mod\ p$.*

Demonstração. Considere o conjunto $F = \{a, 2a, 3a, ..., (p-1) \cdot a\}$. Sabe-se que qualquer elemento pertencente a F é menor ou igual a $(p-1) \cdot a$, portanto, nenhum elemento do conjunto é divisível por p. Além disso, quaisquer dois elementos distintos de F são incongruentes módulo p, visto que como $(a, p) = 1$, para que $aj \equiv ak \mod p$ (supondo que j, k pertençam ao conjunto F), teríamos pela Proposição 2.15 que $j \equiv k \mod p$, o que implica que $j = k$. Esta igualdade não pode ser considerada, porque claramente podemos fazer uma relação biunívoca entre este conjunto apresentado e o *sistema reduzido de resíduos módulo p*. Para evidenciar esta relação, vamos estabelecer uma congruência módulo p entre o conjunto F e o *sistema reduzido de resíduos* módulo p, conforme veremos a seguir:

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

Esta relação quando simplificada, fica:

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p.$$

Considerando que $((p-1)!, p) = 1$, pela Proposição 2.15, podemos realizar o cancelamento nos dois membros da congruência, ficando com

$$a^{p-1} \equiv 1 \bmod p,$$

o que conclui a demonstração. □

Este resultado nos apresenta um teste para descobrir números não-primos. Pois, considerando $a, m \in \mathbb{N}$ tais que $m > 1$ e $(a, m) = 1$, se $m \nmid a^{m-1} - 1$, então m não é primo. Temos também uma consequência desse Teorema, que também é chamado de Pequeno Teorema de Fermat, como veremos a seguir.

Corolário 3.1. *Seja p um número primo. Então, temos que $p \mid a^p - a$, $\forall a \in \mathbb{Z}$.*

Demonstração. Pelo Teorema 3.2, temos que $a^{p-1} \equiv 1 \bmod p$. Sabemos que $a \equiv a \bmod p$. Temos, então, pela Proposição 2.13, que $a^{p-1} \cdot a \equiv 1 \cdot a \bmod p$. Logo, $a^p \equiv a \bmod p$. □

Observação 3.2. *Verifique que, no Colorário 3.1, se fizermos $a = 2$, teremos justamente o caso particular que foi apresentado no início do capítulo de que se p é primo, então $p \mid 2^p - 2$.*

Dito isto, temos esta subseção por finalizada e iniciaremos na próxima subseção um estudo acerca do Teorema de Euler.

3.3 Teorema de Euler

Euler é um dos matemáticos mais conhecidos e falados na atualidade, isto porque ele reuniu uma série de contribuições ao longo do tempo para a construção da Matemática que temos hoje. O grande matemático suíço tinha uma mente extraordinária e suas contribuições foram nas mais variadas áreas, como por exemplo: Teoria das Funções, Teoria das Partições e Mecânica.

Como já foi mencionado na Seção 2.1, Euler se comunicava com Goldbach acerca dos resultados apresentados por Fermat sobre os números primos. E nesta subseção, trataremos do Teorema de Euler que é, basicamente, uma generalização do Pequeno Teorema de Fermat.

Para iniciar esta subseção, como saber se $aX \equiv 1 \bmod m$ tem alguma solução em X? A resposta para esse questionamento pode ser encontrada através da proposição descrita abaixo:

Proposição 3.1. *Dados $a, m \in \mathbb{Z}$ com $m > 1$, temos que $aX \equiv 1$ mod m possui solução se, e somente se, $(a, m) = 1$. E se x_0 for uma solução, dizemos que x também é uma solução se $x \equiv x_0$ mod m.*

Demonstração. A congruência $aX \equiv 1 \bmod m$ tem solução x_0 se, e somente se, $m \mid ax_0 - 1$. Encontrar essa solução é equivalente a solucionar a equação $aX - mY = 1$ e, por isso, tem solução se, e somente se, $(a, m) = 1$. Da mesma forma, se x_0 e x são soluções da congruência $aX \equiv 1 \bmod m$, então $ax \equiv ax_0 \bmod m$. Como $(a, m) = 1$, temos, pela Proposição 2.15 que $x \equiv x_0 \bmod m$.

□

Utilizaremos a notação $\varphi(m)$ para denotar a quantidade de elementos de um *sistema reduzido de resíduos* módulo m, tal que $m > 1$. Nesse caso, de acordo com a Definição 2.6, será um *sistema reduzido de resíduos* formado apenas por todos os números naturais entre 0 e $m-1$ que são primos com m. Se colocarmos $\varphi(1) = 1$, podemos definir a função

$$\varphi : \mathbb{N} \to \mathbb{N},$$

que chamaremos de *Phi de Euler*. Além disso, pela definição de *sistema reduzido de resíduos*, nós temos que

$$\varphi(m) \leq m - 1.$$

Podemos ter $\varphi(m) = m - 1$ porque se m for um primo, então para todo r que seja um resíduo módulo m teremos que $(m, r) = 1$, ou seja, todos os restos possíveis serão contabilizados no SRR. E podemos ter $\varphi(m) < m-1$, porque se m não for primo, teremos pelo menos um r tal que $(m, r) \neq 1$, o que faz com que o número de elementos do SRR seja menor que $m - 1$.

Exemplo 3.2. $\varphi(12) = 4$, *pois um exemplo de sistema reduzido de resíduos módulo* 12 *pode ser* $\{1, 5, 7, 11\}$ *e* $\varphi(5) = 4$, *pois um exemplo de sistema reduzido de resíduos módulo* 5 *pode ser* $\{1, 2, 3, 4\}$.

A função *Phi de Euler* é muito importante para a Teoria dos Números, portanto vamos apresentar algumas proposições abaixo que se utilizam dela.

Proposição 3.2. *Se* $\{r_1, r_2, ..., r_{\varphi(m)}\}$ *for um sistema reduzido de resíduos módulo* m *e* $(a, m) = 1$ *para todo* $a \in \mathbb{Z}$, *então* $\{ar_1, ar_2, ..., ar_{\varphi(m)}\}$ *também é um sistema reduzido de resíduos.*

Demonstração. Seja $\{r_1, r_2, ..., r_{\varphi(m)}\}$ um *sistema reduzido de resíduos* módulo m e suponha que $\{a_1, a_2, ..., a_m\}$ também seja um outro *sistema reduzido de resíduos* módulo m retirado do sistema anterior apresentado. Como $(a, m) = 1$ e $(r_i, m) = 1$, temos que $(ar_i, m) = 1$. Isto nos diz que se tomarmos $ar_i \equiv ar_j \bmod m$, teremos, pela Proposição 2.15, $r_i \equiv r_j \bmod m$, portanto $i = j$, o que conclui a nossa demonstração, já que $\{r_1, r_2, ..., r_{\varphi(m)}\}$ é um *sistema reduzido de resíduos.* □

Teorema 3.3 (Teorema de Euler)**.** *Seja* $(a, m) = 1$*, com* $a, m \in \mathbb{Z}$*, tal que* $m > 1$*. Então,* $a^{\varphi(m)} \equiv 1$ *mod* m*.*

Demonstração. Considerando $\{r_1, r_2, ..., r_m\}$ um sistema reduzido de resíduos módulo m, então, pela Proposição 3.2, temos que $\{ar_1, ar_2, ..., ar_{\varphi(m)}\}$ também é um sistema reduzido de resíduos módulo m. Dessa forma,

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \bmod m.$$

Em virtude disso,

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi(m)} \equiv a^{\varphi(m)} r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \bmod m.$$

E como $(r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)}, m) = 1$, então, $a^{\varphi(m)} \equiv 1 \bmod m$. □

Observação 3.3. *Para relacionar o Teorema de Euler com o Pequeno Teorema de Fermat, basta tomar* $\varphi(p) = p - 1$*, com* p *primo, ficando, assim, com* $a^{p-1} \equiv 1$ *mod* p*.*

3.4 Teorema de Wilson

O Teorema de Wilson foi apresentado pelo aluno John Wilson (1741-1793) ao seu professor Edward Waring (1734-1798), matemático e autor do livro *Meditationes Algebraicae*, no qual este e outros teoremas foram apresentados. Através de seus cálculos, Wilson descobriu que se p é um número primo, então $p \mid (p-1)! + 1$. Porém, nem ele e nem o seu professor foram capazes de provar este enunciado.

Sabe-se que até os dias atuais, não existe uma fórmula que gere todos os números primos. Waring atribuiu a esta situação, o fato de não ter conseguido provar o teorema proposto por Wilson. Gauss, ao saber da situação, disse que neste tipo de demonstração a ideia que o número primo representava era mais importante que a notação.

E, de fato, quem o provou pela primeira vez foi o matemático Lagrange (1736-1813), afirmando e demonstrando também que a recíproca do chamado "Teorema de Wilson" é verdadeira. Contudo, muitos matemáticos acreditam que o teorema deveria ter sido atribuído a Leibniz que, devido a algumas evidências, aparentemente sabia do resultado há aproximadamente um século antes, mas nunca havia publicado nada a respeito.

Agora veremos uma proposição que será utilizada para provar o Teorema de Wilson e, em seguida, demonstraremos o referido teorema.

Proposição 3.3. *Sendo* $a, p \in \mathbb{Z}$ *com* p *primo, temos que* a *é o seu próprio inverso modular se, e somente se,* $a \equiv 1$ *mod* p *ou* $a \equiv -1$ *mod* p*.*

Demonstração. Se considerarmos que a é o seu próprio inverso mod p, então $a^2 \equiv 1 \bmod p$, ou seja, $p \mid (a^2 - 1)$, ou simplesmente, $p \mid (a+1)(a-1)$. Alinhando esta informação ao fato de que p é primo, temos que p divide apenas um dos fatores, logo, $p \mid (a+1)$ ou

$p \mid (a-1)$. Este resultado implica que $a \equiv 1 \bmod p$ ou $a \equiv -1 \bmod p$. Reciprocamente, se $p \mid (a+1)$ ou $p \mid (a-1)$, podemos considerar que $p \mid (a+1)(a-1)$, ou simplesmente que $p \mid (a^2-1)$, logo, $a^2 \equiv 1 \bmod p$. □

Observação 3.4. *Ou seja, o inverso de a mod p é* a^{-1}*, já que* $a \cdot a^{-1} \equiv 1$ *mod p.*

Teorema 3.4 (Teorema de Wilson)**.** *Sendo p um número primo, então* $(p-1)! \equiv -1$ *mod p.*

Demonstração. O enunciado é válido para $p = 2$ e $p = 3$, pois é facilmente verificável que $(2-1)! \equiv -1 \bmod 2$ e $(3-1)! \equiv -1 \bmod 3$. Como é sabido, a congruência $aX \equiv 1 \bmod p$ tem apenas uma solução para todo $k \in \{1, 2, 3, ..., (p-1)\}$, e como de acordo com a Proposição 3.3, dos elementos pertencentes ao conjunto, apenas o 1 e o $(p-1)$ são seus próprios inversos módulo p, podemos agrupar os elementos restantes em $(p-3)/2$ pares cujo o produto será congruente a 1, resultando em

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

Agora, se multiplicarmos ambas as partes componentes da congruência por $(p-1)$, ficamos com

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

E simplificando este resultado, temos

$$(p-1)! \equiv (p-1) \equiv -1 \bmod p,$$

ou simplesmente,

$$(p-1)! \equiv -1 \bmod p,$$

como queríamos demonstrar. □

Agora que os teoremas foram apresentados, daremos este capítulo por encerrado e começaremos o próximo discutindo sobre os Resíduos Quadráticos.

Capítulo 4

Resíduos Quadráticos

Neste capítulo, abordaremos os Resíduos Quadráticos. Veremos a sua definição e seus principais resultados, que serão importantes para posteriormente estudarmos a representação de inteiros como soma de quadrados.

4.1 Resíduos Quadráticos

Para iniciarmos, vamos nos ater à definição de *resíduos quadráticos* dada a seguir.

Definição 4.1. *Considerando $a, m \in \mathbb{Z}$, com $m > 0$, dizemos que a é um resíduo quadrático módulo m, se a congruência $x^2 \equiv a \ mod\ m$ tiver solução. Se a congruência $x^2 \equiv a \ mod\ m$ não tiver solução, dizemos que a é um resíduo não-quadrático ou que a não é um resíduo quadrático módulo m.*

Exemplo 4.1. *Dizemos que 1 é um resíduo quadrático módulo 3, já que $2^2 \equiv 1 \ mod\ 3$. Já o 2 não é um resíduo quadrático módulo 4, visto que não existe um x tal que $x^2 \equiv 2 \ mod\ 4$.*

Desta definição decorrem importantes teoremas que serão descritos a seguir.

Teorema 4.1. *Dados $a, p, x \in \mathbb{Z}$, tal que p é um primo maior que 2 e $(a, p) = 1$, se a congruência $x^2 \equiv a \ mod\ p$ tem solução, então tem exatamente duas soluções incongruentes entre si.*

Demonstração. Supondo que a congruência tenha x_1 como solução, então, precisaremos considerar $-x_1$ também como solução, pois $(x_1)^2 = (-x_1)^2 \equiv a \bmod p$. Devemos mostrar, então, que estas duas soluções são incongruentes módulo p. Se tivéssemos que $x_1 \equiv -x_1 \bmod p$, então poderíamos dizer que $2x_1 \equiv 0 \bmod p$, porém, p é ímpar e $p \nmid x_1$ (visto que $p \nmid a$ e $p \mid (x_1^2 - a)$), portanto, não é possível que $x_1 \equiv -x_1 \bmod p$. Para finalizar, precisamos mostrar que as soluções incongruentes são apenas duas. Vamos supor que y

seja uma solução da congruência $x^2 \equiv a \bmod p$. Com isso, temos que $y^2 \equiv a \bmod p$. Isto implica que $x_1^2 \equiv y^2 \equiv a \bmod p$, assim, resultando que

$$x_1^2 - y^2 = (x_1 + y) \cdot (x_1 - y) \equiv 0 \bmod p.$$

Isto nos diz que $p \mid (x_1 + y)$ ou $p \mid (x_1 - y)$, sendo, dessa forma, que $y \equiv -x_1 \bmod p$ ou $y \equiv x_1 \bmod p$, nos mostrando que existem apenas duas soluções incongruentes caso a congruência $x^2 \equiv a \bmod p$ tenha solução. □

Exemplo 4.2. *Considere a congruência* $x^2 \equiv a \ mod\ 13$. *Se substituirmos* x *pelos possíveis restos numa divisão por* 13 *e descobrirmos os valores de* a, *temos*

$$0^2 \equiv 0 \ mod\ 13$$

$$1^2 \equiv 1 \ mod\ 13 \qquad 7^2 \equiv 10 \ mod\ 13$$
$$2^2 \equiv 4 \ mod\ 13 \qquad 8^2 \equiv 12 \ mod\ 13$$
$$3^2 \equiv 9 \ mod\ 13 \qquad 9^2 \equiv 3 \ mod\ 13$$
$$4^2 \equiv 3 \ mod\ 13 \qquad 10^2 \equiv 9 \ mod\ 13$$
$$5^2 \equiv 12 \ mod\ 13 \qquad 11^2 \equiv 4 \ mod\ 13$$
$$6^2 \equiv 10 \ mod\ 13 \qquad 12^2 \equiv 1 \ mod\ 13$$

Aqui, observa-se que $12 \not\equiv 1 \ mod\ 13$, $2 \not\equiv 11 \ mod\ 13$, $3 \not\equiv 10 \ mod\ 13$, $4 \not\equiv 9 \ mod\ 13$, $5 \not\equiv 8 \ mod\ 13$ *e* $6 \not\equiv 7 \ mod\ 13$, *conforme foi enunciado no Teorema 4.1.*

Os próximos três teoremas a serem apresentados trazem alguns resultados sobre as congruências módulo p, com p primo, envolvendo polinômios.

Teorema 4.2 (Lagrange)**.** *Considere o polinômio* $f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_2 x^2 + c_1 x + c_0$, *no qual* $c_n, p \in \mathbb{Z}$, p *é primo e* $(c_n, p) = 1$. *Diante do estabelecido, temos que a congruência* $f(x) \equiv 0 \ mod\ p$ *tem no máximo* n *soluções, sendo que quando* $n > p$, *ela tem no máximo* p *soluções distintas por ser uma congruência módulo* p.

Demonstração. Esta demonstração será realizada por meio de indução em n, o grau do polinômio $f(x)$. Primeiro, para $n = 1$ o nosso polinômio fica

$$f(x) = c_1 x + c_0 \equiv 0 \bmod p.$$

Neste caso, como $(c_1, p) = 1$, pelo Teorema 2.3, isso nos diz que a congruência possui apenas uma solução, o que significa que o enunciado é válido para $n = 1$. Agora, iremos assumir que o teorema é válido para $n-1$. Iremos provar por contradição, ao supor que a congruência $f(x) \equiv 0 \bmod p$ tenha $n+1$ soluções incongruentes. Para tanto chamaremos de $x_0, x_1, x_2, \ldots, x_n$ as $n+1$ soluções para esta congruência dada.

Logo se fizermos $f(x) - f(x_0)$, temos que

$$f(x) - f(x_0) = c_n(x^n - x_0^n) + c_{n-1}(x^{n-1} - x_0^{n-1}) + \ldots + c_1(x - x_0),$$

ou seja,

$$f(x) - f(x_0) = (x - x_0)h(x).$$

Isto ocorre pois a Prosposição 2.8 diz que $(x^i - x_0^i)$ é divisível por $(x - x_0)$, para todo i inteiro, sendo $i = 1, 2, 3, \ldots, n$ e que neste caso, $h(x)$ representa um polinômio de grau $n-1$, sendo que c_n é o coeficiente de x^{n-1}. Dessa forma, como sabemos que $f(x_k) \equiv f(x_0)$ mod p, temos

$$f(x_k) - f(x_0) = (x_k - x_0)h(x_k) \equiv 0 \text{ mod } p.$$

Ou seja, para $k \neq 0$, teremos $h(x_k) \equiv 0$ mod p, pois, de acordo com a Proposição 2.15, $x_k \not\equiv x_0$ mod p, se $x_k \neq x_0$. Portanto, a congruência $h(x) \equiv 0$ mod p possui n soluções incongruentes módulo p, o que é uma contradição já que o maior grau de $h(x)$ é $n - 1$ e $(c_n, p) = 1$. Sendo assim, concluímos que $f(x)$ não pode ter mais que n soluções incongruentes módulo p. □

Teorema 4.3. *Dado um polinômio $f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_2 x^2 + c_1 x + c_0$ de grau n, com os coeficientes inteiros, se a congruência $f(x) \equiv 0$ mod p, com p sendo um primo, tiver mais que n soluções, então todos os coeficientes deste polinômio são divisíveis por p.*

Demonstração. Para realizar esta prova, suponhamos que existe um coeficiente de $f(x)$ que não é divisível por p. Para tanto, consideraremos j o maior índice possível que faça com que o coeficiente c_j não seja divisível por p. Desta forma, teremos que

$$c_j x^j + c_{j-1}x^{j-1} + \ldots + c_1 x + c_0 = f(x) - c_n x^n - \ldots - c_{j+1}x^{j+1} \equiv 0 \text{ mod } p.$$

Devido ao fato da congruência apresentada ter mais que n soluções, temos pelo Teorema 4.2 que há uma contradição, visto que p precisa dividir c_j (o que nos diz que $(c_j, p) \neq 1$), como queríamos demonstrar. □

Teorema 4.4. *Seja $f(x) = (x-1)\cdot(x-2)\cdot\ldots\cdot(x-p+1) - x^{p-1} + 1$ um polinômio. Se p for primo, então p divide todos os coeficientes do polinômio $f(x)$.*

Demonstração. Para esta prova, considere $h(x) = (x-1)\cdot(x-2)\cdot\ldots\cdot(x-(p-1))$. É notório que teremos $1, 2, 3, \ldots, p-1$ como soluções de $h(x)$. Em virtude destes fatos, podemos dizer que estas raízes do polinômio $h(x)$ também são soluções para a congruência $h(x) \equiv 0$ mod p. Sabe-se que essas soluções são primos com p, o que nos possibilita dizer, pelo Teorema 3.2, que elas são soluções de $g(x) = x^{p-1} - 1 \equiv 0$ mod p. Então, temos na verdade que $f(x) = h(x) - g(x)$ é um polinômio que possui $p-1$ soluções e grau $p-2$, o que pelo Teorema 4.3, nos diz que p divide todos os coeficientes de $f(x)$. □

O próximo teorema a ser apresentado trará um resultado muito importante sobre resíduos quadráticos de um primo, pois ele facilita muito os cálculos e será utilizado para embasar outros teoremas.

Teorema 4.5. *Considere $A = \{1, 2, 3, \ldots, p-1\}$. Se p é um número primo maior que 2, então, dentre os elementos de A, $(p-1)/2$ são resíduos quadráticos módulo p e $(p-1)/2$ não são.*

Demonstração. Para esta demonstração, vamos elevar os primeiros $(p-1)/2$ elementos de A ao quadrado, ficando com

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Agora, mostraremos que estes números elevados ao quadrado são incongruentes módulo p. Para isso, consideraremos x e y tais que $1 \leq x \leq (p-1)/2$ e $1 \leq y \leq (p-1)/2$ e vamos supor também que $x^2 \equiv y^2 \bmod p$. Devido a isso, temos que $x^2 - y^2 \equiv 0 \bmod p$, ou seja, $(x+y)(x-y) \equiv 0 \bmod p$, nos indicando que $p \mid (x+y)(x-y)$. Mas é necessário excluir a possibilidade de que $p \mid (x+y)$, visto que $x + y < p$. Logo, concluímos que $p \mid (x-y)$, o que implica que $x \equiv y \bmod p$ e, portanto, $x = y$. Conclui-se, assim, que esses $(p-1)/2$ elementos de A elevados ao quadrado são incongruentes módulo p. É notório que quando k percorre o conjunto $\{1, 2, 3, \ldots, (p-1)/2\}$, $p - k$ percorre o conjunto

$$\left\{\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1\right\}.$$

Ademais, como pode-se estabelecer a relação de congruência

$$(p-k)^2 \equiv p^2 - 2kp + k^2 \equiv 0^2 - 2 \cdot k \cdot 0 + k^2 \equiv k^2 \bmod p,$$

conclui-se que os resíduos quadráticos pertencem às classes de congruências que contém os quadrados

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Isto conclui a demonstração de que dentre os números $\{1, 2, , 3, \ldots, p-1\}$, temos que $(p-1)/2$ são resíduos quadráticos e $(p-1)/2$ não são. □

Exemplo 4.3. *Vamos testar este teorema para $x^2 \equiv a$ mod 11. Assim temos:*

$0^2 \equiv 0$ *mod* 11*]*
$1^2 \equiv 1$ *mod* 11
$2^2 \equiv 4$ *mod* 11
$3^2 \equiv 9$ *mod* 11
$4^2 \equiv 5$ *mod* 11
$5^2 \equiv 3$ *mod* 11
$6^2 \equiv 3$ *mod* 11
$7^2 \equiv 5$ *mod* 11
$8^2 \equiv 9$ *mod* 11
$9^2 \equiv 4$ *mod* 11
$10^2 \equiv 1$ *mod* 11

Percebe-se que os resíduos quadráticos mod 11 são {1,2,4,5,9}, ou seja, temos 5 resíduos. E, de fato, $(p-1)/2 = (11-1)/2 = 10/2 = 5$.

Teorema 4.6. *Seja a congruência $x^2 \equiv -1$ mod p, com p sendo um primo. Esta congruência apresenta solução se, e somente se, $p = 2$ ou $p \equiv 1$ mod 4.*

Demonstração. Se tivermos $p = 2$, teremos $x \equiv -1 \bmod p$ e sabemos que $x = 1$, pois $1^2 \equiv -1 \bmod 2$. Agora, é importante pensar como seria a solução para $p \equiv 1 \bmod 4$. Para tanto, sendo p um número primo, consideraremos o Teorema de Wilson que diz que $(p-1)! \equiv -1 \bmod p$. Nós podemos escrever $(p-1)!$ separando-o em duas partes, como descrito a seguir:

$$\big(1 \cdot 2 \cdot 3 \cdot \ldots \cdot j \cdot \ldots \cdot (p-1)/2\big)\big((p+1)/2 \cdot \ldots \cdot (p-j) \cdot \ldots \cdot (p-2) \cdot (p-1)\big) \equiv -1 \bmod p.$$

O produto foi separado em duas partes com o mesmo número de fatores. É possível reunir pares, sendo que para cada fator j na primeira parte da separação acima, temos um fator $(p-j)$ na segunda parte. Ao considerar isso, podemos escrever o Teorema de Wilson como:

$$\prod_{j=1}^{(p-1)/2} j(p-j) \equiv -1 \bmod p.$$

Sabe-se que $j(p-j) \equiv -j^2 \bmod p$, então, temos que:

$$-1 \equiv \prod_{j=1}^{(p-1)/2} (-j^2) \equiv (-1)^{(p-1)/2} \left(\prod_{j=1}^{(p-1)/2} j \right)^2 \bmod p.$$

Sendo $p \equiv 1 \bmod 4$, tem-se que $(p-1)/2$ é par. Logo temos que

$$x = \prod_{j=1}^{(p-1)/2} j = \left(\frac{p-1}{2} \right)!$$

representa uma solução da congruência $x^2 \equiv -1 \bmod p$. Agora, consideremos que a congruência $x^2 \equiv -1 \bmod p$ tenha solução e $p > 2$. Se elevarmos os dois membros a $(p-1)/2$, ficamos com:

$$(x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \bmod p.$$

Já que $(x^2)^{(p-1)/2} \equiv x^{(p-1)} \bmod p$ e $p \nmid x$ já que $x^2 \equiv -1 \bmod p$, temos pelo Teorema 3.2 que

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

Então $(p-1)/2$ é par e $p \equiv 1 \bmod 4$. □

Exemplo 4.4. *Note que $13 \equiv 1$ mod 4. Portanto, $x^2 \equiv -1$ mod 13 tem solução, como vimos no Exemplo 4.2. De fato, por este exemplo, temos que $5^2 \equiv 8^2 \equiv 12 \equiv -1$ mod 13. Já $11 \not\equiv 1$ mod 4, e o Exemplo 4.3 evidencia que, de fato, não existe x tal que $x^2 \equiv -1 \equiv 10$ mod 11.*

4.2 Símbolo de Legendre e Critério de Euler

Nesta seção, apresentaremos uma notação que facilita a compreensão de muitos resultados, que é o chamado *Símbolo de Legendre*. Veremos, assim, a sua definição e a sua relação com uma importante ferramenta chamada Critério de Euler.

Definição 4.2. *Sejam $a, p \in \mathbb{Z}$, tais que $(a,p) = 1$ e p é um primo ímpar. Chamamos $\left(\frac{a}{p}\right)$ de Símbolo de Legendre de a com p, em que*

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

Exemplo 4.5. *Sabe-se que $x^2 \equiv 1 \ mod\ 5$ e $x^2 \equiv 4 \ mod\ 5$ possuem soluções (1 e 4; 2 e 3, respectivamente), mas $x^2 \equiv 2 \ mod\ 5$ e $x^2 \equiv 3 \ mod\ 5$ não possuem. Se representarmos estas informações através do Símbolo de Legendre, temos que*

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1 \text{ e } \left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

A seguir veremos o Critério de Euler, que é um resultado construído a partir do Símbolo de Legendre e é crucial para o desenvolvimento deste trabalho.

Teorema 4.7 (Critério de Euler)**.** *Sejam $a, p \in \mathbb{Z}$ tais que p é um primo ímpar e $(a,p) = 1$. Então*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \ mod\ p.$$

Demonstração. Para realizar esta prova, vamos supor, a princípio, que $\left(\frac{a}{p}\right) = 1$. Isto significa que a congruência $x^2 \equiv a \bmod p$ tem solução. Então, se considerarmos y como uma solução desta congruência, teremos que $(p,y) = 1$ visto que $p \mid (y^2 - a)$ e $p \nmid a$. Desta forma, pelo Pequeno Teorema de fermat, temos que $y^{p-1} \equiv 1 \bmod p$, ou seja,

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

Isto prova que o teorema é válido para $\left(\frac{a}{p}\right) = 1$. Agora, consideraremos $\left(\frac{a}{p}\right) = -1$. Para tanto, vamos nos ater ao resultado anterior de que se a for um resíduo quadrático mod p, então $a^{(p-1)/2} \equiv 1 \bmod p$. Sabe-se que, pelo Teorema 4.2, a congruência $f(x) = a^{(p-1)/2} - 1 \equiv 0 \bmod p$ tem, no máximo, $(p-1)/2$ soluções incongruentes módulo p. Relacionando isto ao fato de que $(p-1)/2$ elementos de $\{1, 2, \ldots, p-1\}$ são resíduos quadráticos e $a^{(p-1)/2} \equiv 1 \bmod p$ para todo resíduo quadrático, teremos que todos esses resíduos serão solução da congruência $f(x) \equiv 0 \bmod p$ e, consequentemente, as $(p-1)/2$ raízes. Por isso, se a não for um resíduo quadrático, então $a^{(p-1)/2} \not\equiv 1 \bmod p$. Ademais, já que

$$a^{p-1} - 1 = (a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) \text{ e } a^{p-1} - 1 \equiv 0 \bmod p, \text{ para } (a, p) = 1,$$

concluímos que $a^{(p-1)/2} \equiv \pm 1 \bmod p$. Sendo assim, caso tenhamos que $\left(\frac{a}{p}\right) = -1$, deveremos ter $a^{(p-1)/2} \equiv -1 \bmod p$. Logo,

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

como queríamos demonstrar. □

Exemplo 4.6. *Para $a = 4$ e $p = 13$, temos que*

$$\left(\frac{4}{13}\right) \equiv 4^{(13-1)/2} \equiv 4^6 \equiv 1 \ mod\ 13,$$

que, de fato, é uma afirmação verdadeira, já que 4 é resíduo quadrático de 13, como vimos no Exemplo 4.2. De maneira similar, para $a = 2$ e $p = 13$, temos que

$$\left(\frac{2}{13}\right) \equiv 2^{(13-1)/2} \equiv 2^6 \equiv -1 \ mod\ 13,$$

que, de fato, é uma afirmação verdadeira, já que 2 não é resíduo quadrático de 13, como vimos no Exemplo 4.2.

Iremos, agora, apresentar a definição de função completamente multiplicativa, com o intuito de enunciar um resultado que envolve este conceito e o Critério de Euler.

Definição 4.3. *Uma função é chamada completamente multiplicativa sempre que tivermos $f(mn) = f(m) \cdot f(n)$, para m e n inteiros quaisquer.*

Teorema 4.8. *Sejam $a, b, p \in \mathbb{Z}$ com $p > 2$ e primo. A função representada pelo Símbolo de Legendre é completamente multiplicativa, o que significa que*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

em que $p \nmid a$ e $p \nmid b$.

Demonstração. Pelo Critério de Euler, temos que:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} \cdot b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p.$$

Sabe-se que o Símbolo de Legendre pode assumir o valor -1 ou 1 e que p é ímpar, logo, temos que a igualdade

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

é verdadeira. □

O presente teorema pode ser interpretado de seguinte maneira: um resíduo não-quadrático, multiplicado por outro resíduo não-quadrático, ambos módulo p, resulta em um resíduo quadrático (já que $(-1)\cdot(-1) = 1$). Da mesma forma, um resíduo quadrático, multiplicado por outro resíduo quadrático, vai resultar em um resíduo quadrático (visto que $1 \cdot 1 = 1$). Por fim, se tivermos um resíduo quadrático multiplicado por um não-quadrático, teremos um resíduo não-quadrático como resultado (pelo fato de que $1 \cdot (-1) = -1$).

Exemplo 4.7. *Fizemos, abaixo, a tabela de multiplicação dos restos não-nulos módulo 7, pondo em vermelho os resíduos quadráticos* ($\overline{1}$, $\overline{2}$ *e* $\overline{4}$)*, e em azul os resíduos não-quadráticos* ($\overline{3}$, $\overline{5}$ *e* $\overline{6}$)*.*

Tabela 4.1: Resíduos da divisão de um inteiro por 7.

$*$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Fonte: elaborada pela autora.

Observe que a coloração evidencia, de maneira mais nítida, o comentário realizado após a demonstração do Teorema 4.8.

Observação 4.1. *A representação usada acima, com uma barra sobre os resíduos, não altera o significado de resíduo que foi apresentado. Esta é apenas uma outra notação algébrica. Nesse caso, se estivermos falando sobre o conjunto dos possíveis restos numa divisão de um inteiro por* m*, temos* $Z_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$.

Teorema 4.9. *Sendo* p *um primo, tal que* $p > 2$*, temos que*

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

Demonstração. De acordo com o Critério de Euler, temos que

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

Então, $\left(\frac{-1}{p}\right) = 1$ quando $(p-1)/2$ for par e $\left(\frac{-1}{p}\right) = -1$, quando $(p-1)/2$ for ímpar. Também sabe-se que existem apenas duas possibilidades para p na congruência usando módulo 4: ou $p \equiv 1 \bmod 4$ ou $p \equiv 3 \bmod 4$. Se $p \equiv 1 \bmod 4$, então $4 \mid (p-1)$, ou

seja, $(p-1)/2$ será par. Se tivermos, ao invés disso, a congruência $p \equiv 3 \bmod 4$, teremos, então, que $4 \mid (p-1-2)$, sendo assim, $p-1-2 = 4k$, para $k \in \mathbb{Z}$. Dessa forma, $p-1 = 4k+2 = 2 \cdot (2k+1)$, o que indica que $(p-1)/2$ é ímpar.

Portanto, para a congruência $p \equiv 1 \bmod 4$, teremos $\left(\frac{-1}{p}\right) = 1$ e para $p \equiv 3 \bmod 4$, teremos $\left(\frac{-1}{p}\right) = -1$, como queríamos demonstrar. □

Exemplo 4.8. *Substituindo $p = 5$ no teorema anterior, ficamos com $\left(\frac{-1}{5}\right) = 1$ porque $5 \equiv 1$ mod 4. Isso, de fato, se verifica, pois*

$$-1 \equiv 4 \equiv 2^2 \ mod\ 5,$$

mostrando que -1 é resíduo quadrático mod 5. Agora, considerando $p = 11$ no teorema anterior, obtemos $\left(\frac{-1}{11}\right) = -1$, porque $11 \equiv -1$ mod 4. Isso ocorre também devido ao fato da congruência

$$-1 \equiv 10 \ mod\ 11$$

ser válida, e já termos visto, no Exemplo 4.3, que 10 não é resíduo quadrático de 11.

Neste capítulo vimos conceitos e desdobramentos importantes para a elaboração do próximo capítulo, que apresenta a representação de inteiros como soma de quadrados. Vimos ferramentas e a forma como elas se relacionam, bem como exemplos que servem para demonstrar a aplicação destes teoremas com a intenção de facilitar o entendimento acerca deles.

Capítulo 5

Representação de Inteiros como Soma de Quadrados

5.1 O Problema de Waring

O matemático inglês Edward Waring (1741-1793), ao estudar acerca dos inteiros, publicou um trabalho no ano de 1770, afirmando que todo inteiro positivo é a soma de, no máximo 4 quadrados, no máximo 9 cubos e no máximo 19 quartas potências. Ele também acreditava que para cada inteiro positivo k, existia um inteiro $g(k)$, de tal forma que qualquer natural n pudesse ser representado como soma de, no máximo, $g(k)$ k-ésimas potências. Isto ficou conhecido como o Problema de Waring, todavia, mesmo que tenha afirmado tais alegações, não conseguiu provar nenhuma delas.

O fato de que todo inteiro pode ser representado como uma soma de no máximo quatro quadrados foi provado por Lagrange, também em 1770. Em 1859, veio à tona a demonstração de que todo inteiro pode ser representado como uma soma de no máximo nove cubos. E, por fim, em 1909, o matemático alemão David Hilbert (1862-1943) resolveu (demonstrou) o Problema de Waring.

Apesar da vastidão de conteúdos a serem trabalhados neste campo de estudo, no presente capítulo, iremos, através de um teorema, abordar apenas a representação de inteiros como soma de quadrados. Para tanto, vamos verificar o teorema abaixo que auxilia nesta prova.

Teorema 5.1. *Sendo p primo, existem $a, b, c \in \mathbb{Z}$ não simultaneamente nulos, de tal forma que a congruência*

$$a^2 + b^2 + c^2 \equiv 0 \ mod\ p$$

é válida.

Demonstração. Se tomarmos $p = 2$, podemos ter $a = b = 1$ e $c = 0$, ou seja, $1^2+1^2+0^2 \equiv 0$ mod 2, o que é verdade. Se considerarmos a congruência $p \equiv 1$ mod 4, podemos tomar

$b = 1, c = 0$ e a como uma solução de $x^2 \equiv -1 \bmod p$ (sendo que o Teorema 4.6 afirma a existência deste referido a). Porém, se considerarmos que $p \equiv 3 \equiv -1 \bmod 4$, tomamos $c = 1$ e podemos confirmar a existência de uma solução para a congruência $a^2 + b^2 \equiv -1 \bmod p$, conforme faremos a seguir. Pelo Teorema 4.5, sabemos que quando p é primo, metade dos seus resíduos são quadráticos e metade não são. Considere, então, d como o menor resíduo não-quadrático positivo módulo p. Sabe-se que 1 é um resíduo quadrático, portanto, $d \geq 2$. Logo, temos (de acordo com os Teoremas 4.8 e 4.9) que:

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

Esta igualdade afirma que $-d$ é um resíduo quadrático módulo p, ou seja, isto nos indica que a congruência $x^2 \equiv -d \bmod p$ possui solução. Considere b inteiro, tal que $b^2 \equiv -d \bmod p$. A ideia é encontrar um a que faça a congruência $a^2 \equiv d - 1 \bmod p$ ser válida. E, de fato, esta congruência possui solução já que $d \geq 2$, $d - 1 < d$ e d é o menor resíduo não-quadrático positivo módulo p. □

O teorema a seguir será o último a ser demonstrado no presente trabalho, nele culmina toda a construção realizada a partir das congruências até aqui.

Teorema 5.2 (Lagrange)**.** *Todo inteiro positivo pode ser representado como uma soma de 4 quadrados.*

Demonstração. Se $p = 2$, temos que $2 = 1^2 + 1^2 + 0^2 + 0^2$. Agora, sendo p um primo ímpar, temos, pelo Teorema 5.1, que $a^2 + b^2 + c^2 \equiv 0 \bmod p$, para a, b e c inteiros. Pode-se reescrever esta congruência de forma que ela fique

$$a^2 + b^2 + c^2 + d^2 = Mp. \tag{5.1}$$

Para isso, $d = 0$ e M é um inteiro. Considerando a equação (5.1), sabe-se que existe m tal que este m é o menor inteiro que satisfaz a equação, ou seja,

$$a^2 + b^2 + c^2 + d^2 = mp.$$

Pela demonstração do Teorema 4.5, e pelo Teorema 5.1, podemos assumir que existem $a, b, c \in [0, m/2)$, de forma que

$$mp = a^2 + b^2 + c^2 + d^2 < 4 \cdot \left(\frac{p}{2}\right)^2 = p^2,$$

e concluímos, desta forma, que $m < p$. Para continuarmos com a prova, será suficiente mostrar que $m = 1$.

Para tanto, consideraremos que $m > 1$. Todavia, isto vai nos fornecer um inteiro $0 \leq m' < m$, o que também vai modificar a representação do inteiro como soma de quadrados para $m'p$, o que contradiz a representação que já tinha sido selecionada. Então, vamos separar em dois casos: m par e m ímpar. Para $m > 1$ e ímpar, temos que da equação

$$a^2 + b^2 + c^2 + d^2 = mp,$$

podemos, escolher no intervalo $[0, m/2)$, a_1, b_1, c_1 e d_1 que tornem verdadeiras as congruências $a_1 \equiv a \bmod m$, $b_1 \equiv b \bmod m$, $c_1 \equiv c \bmod m$ e $d_1 \equiv d \bmod m$. Sendo assim, temos a congruência $a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv 0 \bmod m$, o que nos garante que existe um m' tal que $m' \geq 0$ e $a_1^2 + b_1^2 + c_1^2 + d_1^2 = m'm$. Sabe-se que os inteiros a_1, b_1, c_1 e d_1 são menores que $m/2$ e, portanto, $m' < m$. Porém, considerar que $m' = 0$ encaminha a prova para uma contradição, já que quando $m' = 0$, temos que $a_1 = b_1 = c_1 = d_1 = 0$, ou seja, $a \equiv b \equiv c \equiv d \equiv 0 \bmod m$. Por esta última expressão, pode-se denotar $a = \alpha m$, $b = \beta m$, $c = \gamma m$, $d = \sigma m$, em que $\alpha, \beta, \gamma, \sigma \in \mathbb{Z}$. Daí, segue que

$$mp = a^2 + b^2 + c^2 + d^2 = m^2(\alpha^2 + \beta^2 + \gamma^2 + \sigma^2),$$

o que implica que $m^2 \mid mp$. Este resultado implica que $m \mid p$, o que é uma contradição, já que $1 < m < p$. Logo, $m' \neq 0$. Sendo assim,

$$\begin{aligned} m^2pm' = (mp)(m'm) &= (a^2 + b^2 + c^2 + d^2)(a_1^2 + b_1^2 + c_1^2 + d_1^2) \\ &= (aa_1 + bb_1 + cc_1 + dd_1)^2 + (ab_1 - ba_1 - cd_1 + dc_1)^2 \\ &\quad + (ac_1 + bd_1 - ca_1 - db_1)^2 + (ad_1 - bc_1 + cb_1 - da_1)^2. \end{aligned} \tag{5.2}$$

É importante ressaltar que a última igualdade de (5.2) garante que o produto de números que podem ser expressos como soma de quatro quadrados também poderá ser representado como uma soma de quatro quadrados.

Retomando a demonstração, como já ficou estabelecido que $a \equiv a_1, b \equiv b_1, c \equiv c_1$ e $d \equiv d_1$ e, portanto, $a^2 \equiv a \cdot a_1$, $b^2 \equiv b \cdot b_1$, $c^2 \equiv c \cdot c_1$ e $d^2 \equiv d \cdot d_1$, todos módulo m, podemos perceber que os quatro últimos termos de (5.2), que estão elevados ao quadrado, são múltiplos de m. De fato, segue que

$$\begin{cases} aa_1 + bb_1 + cc_1 + dd_1 \equiv a^2 + b^2 + c^2 + d^2 \equiv mp \equiv 0 \bmod m \\ ab_1 - ba_1 - cd_1 + dc_1 \equiv ab - ba - cd + dc \equiv 0 \bmod m \\ ac_1 + bd_1 - ca_1 - db_1 \equiv ac + bd - ca + db \equiv 0 \bmod m \\ ad_1 - bc_1 + cb_1 - da_1 \equiv ad - bc + cb - da \equiv 0 \bmod m \end{cases}.$$

Isto valida a existência de inteiros $\overline{a}, \overline{b}, \overline{c}, \overline{d}$ que tornam a igualdade abaixo verdadeira:

$$m^2pm' = (\overline{a}m)^2 + (\overline{b}m)^2 + (\overline{c}m)^2 + (\overline{d}m)^2.$$

Logo, temos que $pm' = \overline{a}^2 + \overline{b}^2 + \overline{c}^2 + \overline{d}^2$, sendo $m' < m$, como já vimos. Por fim, é necessário mostrar que para $m > 1$ e par, também encontraremos $\overline{m} < m$, sendo $\overline{m}p$ uma soma de quatro quadrados.

Para m par e maior que 1, temos que todos os inteiros a, b, c e d são necessariamente todos pares, todos ímpares ou dois pares e dois ímpares. Porém, para qualquer um destes três casos, podemos ter que $a \equiv b \bmod 2$ e $c \equiv d \bmod 2$, o que nos possibilita organizar da seguinte maneira:

$$p \cdot \frac{m}{2} = \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2$$

Sendo assim, fazendo $\overline{m} = m/2 < m$, conseguimos representar $\overline{m}$ como soma de quatro quadrados. Portanto, concluímos que $m = 1$. Dessa forma, se tivermos um p primo, ele pode ser expresso como soma de quatro inteiros elevados cada um ao quadrado.

Pelo Teorema Fundamental da Aritmética, podemos escrever qualquer número inteiro n como um produto de fatores primos.

Ou seja,

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} \cdot p_n,$$

sendo $p_1, p_2, ...p_n \in \mathbb{Z}$ primos. E como um primo p qualquer pode ser escrito como soma de quatro quadrados, temos que

$$\begin{aligned} p_1 &= a_1^2 + b_1^2 + c_1^2 + d_1^2 \\ p_2 &= a_2^2 + b_2^2 + c_2^2 + d_2^2 \\ &\vdots \\ p_{n-1} &= a_{n-1}^2 + b_{n-1}^2 + c_{n-1}^2 + d_{n-1}^2 \\ p_n &= a_n^2 + b_n^2 + c_n^2 + d_n^2, \end{aligned}$$

o que nos diz que o inteiro n também pode ser representado conforme a seguir:

$$n = (a_1^2+b_1^2+c_1^2+d_1^2)\cdot(a_2^2+b_2^2+c_2^2+d_2^2)\cdot\ldots\cdot(a_{n-1}^2+b_{n-1}^2+c_{n-1}^2+d_{n-1}^2)\cdot(a_n^2+b_n^2+c_n^2+d_n^2).$$

Pela última igualdade de 5.2, temos que quando multiplicamos um soma de quatro quadrados por outra soma de quatro quadrados, o resultado também é uma soma de quatro quadrados. Portanto, n é uma soma de quatro quadrados, como queríamos demonstrar. □

No próximo capítulo, serão apresentadas as conclusões acerca do trabalho, considerando a trajetória do Capítulo 2 até o Capítulo 5.

Capítulo 6

Conclusões e Perspectivas

O presente trabalho teve o intuito de pesquisar sobre a Representação de Inteiros como Soma de Quadrados. E apesar de conhecermos outras informações acerca do tema, como, o fato de alguns números, em específico, poderem ser, por exemplo, escritos como a soma de dois quadrados, o pretendido foi, de fato, falar do Teorema de Lagrange sobre Representação de Inteiros como Soma de Quadrados, que apresenta um resultado que abrange todos os inteiros.

Para alcançarmos esse fim, foi necessário falar sobre as congruências módulo m, porque elas são essenciais durante todo o processo. Além do seu conteúdo histórico apresentando a contribuição dos mais variados matemáticos e suas respectivas relações com o assunto, as congruências apresentam ferramentas muito interessantes para a construção desta pesquisa, como o Pequeno Teorema de Fermat, o Teorema de Euler e o Teorema de Wilson. Também abordamos os resíduos quadráticos e o Símbolo de Legendre, que trazem um aprofundamento direto no tema e conduz diretamente para o referido Teorema de Lagrange.

Dentre as obras citadas, as mais utilizadas para elaboração desta pesquisa foram Santos (2009) e Hefez (2016). Além disso, o procedimento para a utilização dessas obras foi o de verificar o que havia sobre o conteúdo em cada uma delas e trazer o que aparentava ser o melhor aspecto de cada uma para a construção deste trabalho.

Conclui-se que a pesquisa está em aberto, visto que ainda há o que se explorar sobre o assunto como, por exemplo, o Teorema A_1 e outras vertentes como a Lei da Reciprocidade Quadrática. Além disso, a experiência de escrever sobre este tema certamente contribuiu de maneira positiva para a minha formação. Ademais, espera-se com este trabalho que os alunos consigam utilizá-lo como referência de estudo sobre o tema ou mesmo como embasamento para elaboração de outras pesquisas na área.

Referências

BURTON, D. M. *Teoria Elementar dos Números*. 7. ed. Janeiro - Brasil: LTC, 2016.

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

MERZBACH, C. B. C. *História da Matemática*. 3. ed. São Paulo - Brasil: Edgard Blucher Ltda, 2012.

O'REGAN, G. *Guide to Discrete Mathematics*. Cham - Switzerland: Springer Nature, 2016.

SANTOS, J. P. O. *Introdução à Teoria dos Números*. 3. ed. Rio de Janeiro - Brasil: SBM, 2009.

Apêndice A

Representação dos 100 primeiros inteiros como soma de quadrados

A seguir, fornecemos uma tabela com a representação mais sucinta como soma de quadrados, para cada um dos cem primeiros inteiros positivos. Por sucinta, entende-se que a soma é realizada com a menor quantidade de somandos possível. Dentre as representações apresentadas, existem, em alguns casos, mais de uma alternativa de escolha de quadrados a somar, como por exemplo, $50 = 5^2 + 5^2 = 7^2 + 1^2$.

$1 = 1^2$
$2 = 1^2 + 1^2$
$3 = 1^2 + 1^2 + 1^2$
$4 = 2^2$
$5 = 2^2 + 1^2$
$6 = 2^2 + 1^2 + 1^2$
$7 = 2^2 + 1^2 + 1^2 + 1^2$
$8 = 2^2 + 2^2$
$9 = 3^2$
$10 = 3^2 + 1^2$
$11 = 3^2 + 1^2 + 1^2$
$12 = 2^2 + 2^2 + 2^2$
$13 = 3^2 + 2^2$
$14 = 3^2 + 2^2 + 1^2$
$15 = 3^2 + 2^2 + 1^2 + 1^2$
$16 = 4^2$
$17 = 4^2 + 1^2$
$18 = 3^2 + 3^2$
$19 = 3^2 + 3^2 + 1^2$
$20 = 4^2 + 2^2$
$21 = 4^2 + 2^2 + 1^2$
$22 = 3^2 + 3^2 + 2^2$
$23 = 3^2 + 3^2 + 2^2 + 1^2$
$24 = 4^2 + 2^2 + 2^2$
$25 = 5^2$
$26 = 5^2 + 1^2$
$27 = 5^2 + 1^2 + 1^2$
$28 = 5^2 + 1^2 + 1^2 + 1^2$
$29 = 5^2 + 2^2$
$30 = 5^2 + 2^2 + 1^2$
$31 = 5^2 + 2^2 + 1^2 + 1^2$
$32 = 4^2 + 4^2$
$33 = 4^2 + 4^2 + 1^2$
$34 = 5^2 + 3^2$
$35 = 5^2 + 3^2 + 1^2$
$36 = 6^2$
$37 = 6^2 + 1^2$
$38 = 6^2 + 1^2 + 1^2$
$39 = 5^2 + 3^2 + 2^2 + 1^2$
$40 = 6^2 + 2^2$

$41 = 5^2 + 4^2$
$42 = 5^2 + 4^2 + 1^2$
$43 = 5^2 + 3^2 + 3^2$
$44 = 6^2 + 2^2 + 2^2$
$45 = 6^2 + 3^2$
$46 = 6^2 + 3^2 + 1^2$
$47 = 6^2 + 3^2 + 1^2 + 1^2$
$48 = 4^2 + 4^2 + 4^2$
$49 = 7^2$
$50 = 5^2 + 5^2$
$51 = 7^2 + 1^2 + 1^2$
$52 = 6^2 + 4^2$
$53 = 7^2 + 2^2$
$54 = 7^2 + 2^2 + 1^2$
$55 = 5^2 + 5^2 + 2^2 + 1^2$
$56 = 6^2 + 4^2 + 2^2$
$57 = 7^2 + 2^2 + 2^2$
$58 = 7^2 + 3^2$
$59 = 5^2 + 5^2 + 3^2$
$60 = 5^2 + 5^2 + 3^2 + 1^2$
$61 = 6^2 + 5^2$
$62 = 7^2 + 3^2 + 2^2$
$63 = 7^2 + 3^2 + 2^2 + 1^2$
$64 = 8^2$
$65 = 7^2 + 4^2$
$66 = 5^2 + 5^2 + 4^2$
$67 = 7^2 + 3^2 + 3^2$
$68 = 8^2 + 2^2$
$69 = 8^2 + 2^2 + 1^2$
$70 = 6^2 + 5^2 + 3^2$
$71 = 7^2 + 3^2 + 3^2 + 2^2$
$72 = 6^2 + 6^2$
$73 = 8^2 + 3^2$
$74 = 7^2 + 5^2$
$75 = 5^2 + 5^2 + 5^2$
$76 = 6^2 + 6^2 + 2^2$
$77 = 6^2 + 5^2 + 4^2$
$78 = 7^2 + 5^2 + 2^2$
$79 = 7^2 + 5^2 + 2^2 + 1^2$
$80 = 8^2 + 4^2$
$81 = 9^2$
$82 = 9^2 + 1^2$
$83 = 9^2 + 1^2 + 1^2$
$84 = 8^2 + 4^2 + 2^2$
$85 = 7^2 + 6^2$
$86 = 7^2 + 6^2 + 1^2$
$87 = 9^2 + 2^2 + 1^2 + 1^2$
$88 = 6^2 + 6^2 + 4^2$
$89 = 8^2 + 5^2$
$90 = 9^2 + 3^2$
$91 = 9^2 + 3^2 + 1^2$
$92 = 6^2 + 6^2 + 4^2 + 2^2$
$93 = 8^2 + 5^2 + 2^2$
$94 = 9^2 + 3^2 + 2^2$
$95 = 7^2 + 6^2 + 3^2 + 1^2$
$96 = 8^2 + 4^2 + 4^2$
$97 = 9^2 + 4^2$
$98 = 7^2 + 7^2$
$99 = 9^2 + 3^2 + 3^2$
$100 = 10^2$

Observando com atenção, percebe-se que todo $k \in \mathbb{N}$ que satisfaz $k \equiv 7 \bmod 8$ precisa necessariamente de quatro quadrados em sua representação. De fato, os únicos resíduos quadráticos mod 8 são 0, 1 e 4, e não podemos representar 7 como soma de apenas três desses números.

Finalmente, apresentamos um resultado, devido ao matemático francês Adrien-Marie Legendre (1752-1833), e o qual não iremos provar por não ser o objetivo deste trabalho, que caracteriza quais números necessitam sempre de quatro quadrados em sua representação:

Teorema A.1 (dos Três Quadrados de Legendre)**.** *Um número natural n pode ser escrito como soma de três quadrados de inteiros se, e somente se, ele não é da forma*

$$n = 4^a(8b + 7),$$

em que a e b são inteiros não-negativos.

Percebamos que todos os números que necessitamos utilizar quatro quadrados na representação se enquadram nesta condição, e mais destacadamente, os que são congruentes a 7 módulo 8 surgem dos variados valores que b assume, mantendo $a = 0$ fixado. Vejamos:

$$\begin{aligned}
7 &= 4^0(8 \cdot 0 + 7) \\
15 &= 4^0(8 \cdot 1 + 7) \\
23 &= 4^0(8 \cdot 2 + 7) \\
28 &= 4^1(8 \cdot 0 + 7) \\
31 &= 4^0(8 \cdot 3 + 7) \\
39 &= 4^0(8 \cdot 4 + 7) \\
47 &= 4^0(8 \cdot 5 + 7) \\
55 &= 4^0(8 \cdot 6 + 7) \\
60 &= 4^1(8 \cdot 1 + 7) \\
63 &= 4^0(8 \cdot 7 + 7) \\
71 &= 4^0(8 \cdot 8 + 7) \\
79 &= 4^0(8 \cdot 9 + 7) \\
87 &= 4^0(8 \cdot 10 + 7) \\
92 &= 4^1(8 \cdot 2 + 7) \\
95 &= 4^0(8 \cdot 11 + 7).
\end{aligned}$$