UNIVERSIDADE ESTADUAL DO CEARÁ – UECE

CENTRO DE CIÊNCIAS E TECNOLOGIA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

PAULO SÉRGIO CORDEIRO LÔBO

NÚMEROS INTEIROS QUE PODEM SER ESCRITOS COMO SOMA DE DOIS QUADRADADOS

FORTALEZA – CEARÁ
2015

PAULO SÉRGIO CORDEIRO LÔBO

NÚMEROS INTEIROS QUE PODEM SER ESCRITOS COMO SOMA DE DOIS QUADRADOS

Dissertação apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para obtenção do titulo de Mestre em Matemática.

Orientador: Prof. Dr. João Montenegro de Miranda

FORTALEZA – CEARÁ
2015

Dados Internacionais de Catalogação na Publicação

Universidade Estadual do Çeará

Sistema de Bibliotecas

Lôbo, Paulo Sérgio Cordeiro .
Números inteiros que podem ser escritos como soma de dois quadrados [recurso eletrônico] / Paulo Sérgio Cordeiro Lôbo. - 2015.
1 CD-ROM: 4 ¾ pol.

CD-ROM contendo o arquivo no formato PDF do trabalho acadêmico com 43 folhas, acondicionado em caixa de DVD Slim (19 x 14 cm x 7 mm).

Dissertação (mestrado profissional) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Mestrado Profissional em Matemática em Rede Nacional, Fortaleza, 2015.
Área de concentração: Matemática.
Orientação: Prof. Dr. João Montenegro de Miranda.

1. Divisibilidade. 2. Máximo Divisor Comum. 3. Números Primos. 4. Congruências. 5. Soma de dois quadrados. I. Título.

PAULO SÉRGIO CORDEIRO LÔBO

NÚMEROS INTEIROS QUE PODEM SER ESCRITOS COMO SOMA DE DOIS QUADRADOS

Dissertação apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para obtenção do titulo de Mestre em Matemática.

Aprovada em: 18 \ 09 \ 2015.

AVALIAÇÃO

Prof. Dr. João Montenegro de Miranda (Orientador)
Universidade Estadual do Ceará – UECE

Prof. Dr. João Marques Pereira.
Universidade Estadual do Ceará – UECE

Prof. Dr. José Robério Rogério
Universidade Federal do Ceará – UFC

Dedico este trabalho a todos que sempre me fizeram acreditar na realização dos meus sonhos e trabalharam muito para que eu pudesse realizá-los.

AGRADECIMENTOS

A Deus, por ser essencial em minha vida, autor de meu destino, meu guia, socorro presente na hora das angústias.

Aos meus pais, irmãos, minha esposa, minhas filhas e a toda minha família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida.

Aos amigos e colegas, pelo incentivo e pelo apoio constante.

Ao professor João Montenegro de Miranda que pacientemente me conduziu ao cumprimento desse trabalho, incentivando, orientando, solicitando melhorias, e, principalmente, por sua disponibilidade para conversar sobre este estudo. Isso tudo só fez aumentar o meu respeito e a minha admiração por esse docente.

Ao nosso coordenador Guilherme Ellery, por ser sempre muito solícito em relação aos nossos pedidos burocráticos e por mostrar a importância deste título.

A todos os professores exemplares do núcleo PROFMAT-UECE que, por suas solicitudes, promoveram nosso melhor aprendizado.

Aos meus amigos “Aline” e “Assis” por toda a ajuda e atenção dispensada a mim durante esse tempo.

Aos meus colegas do PROFMAT, que tornaram o ambiente agradável, descontraído, com muita colaboração e estudo.

Ao PROFMAT, pela grande oportunidade de cursar um mestrado.

À CAPES pela bolsa de estudo que me foi concedida.

”Para ser grande, sê inteiro: nada teu exagera ou exclui. Sê todo em cada coisa. Põe quanto és no mínimo que fazes. Assim em cada lago a lua toda brilha, porque alta vive.”

(Fernando Pessoa)

RESUMO

Este trabalho tem como objetivo exibir condições para que se possa garantir quando um número inteiro poderá ser representado como uma soma de dois quadrados. Para isto tornou-se necessária a apresentação de algumas definições como, por exemplo, a de divisibilidade, a de máximo divisor comum, a de números primos, a de congruências e a de demonstrações de determinados teoremas. O teorema de Fermat, o de Wilson e o de Thue foram utilizados como ferramentas na demonstração do objetivo principal que é a representação de um número inteiro como soma de dois quadrados. Essa demonstração será feita em um nível acessível ao estudante do ensino médio sem fugir do rigor dos conceitos matemáticos.

Palavras-chave: Divisibilidade, Máximo Divisor Comum, Números Primos, Congruências, Soma de Dois Quadrados.

ABSTRACT

This paper aims to show conditions can be ensured when a integer can be represented as a sum of two squares. For this become necessary to present some definitions, for example, divisibility, the greatest common divisors, the prime numbers, the congruence and the statements of certain theorems. Fermat's theorem, the Wilson and Thue were used in order to display the main objective is to obtain a whole number as a sum of two squares. This demonstration will be made at a level accessible to high school student without escape the rigor of Mathematical concepts.

Key-words: Divisibility, Greatest Common Divisors, Prime Numbers, Congruencies, Sum of Two Squares.

SUMÁRIO

1 INTRODUÇÃO

Desde a antiguidade, o homem utiliza a matemática para facilitar a vida e organizar a sociedade. Muitos povos antigos, entre eles os gregos, desenvolveram uma teoria dos números, orientados por critérios matemáticos no sentido amplo da palavra. Os gregos descobriram as leis básicas da aritmética, tinham conhecimento sobre vários assuntos da matemática, entre eles: a divisão euclidiana, números primos, o cálculo do máximo divisor comum e o mínimo múltiplo comum e principalmente a geometria plana.

A Teoria dos Números tem sido uma área interessante para estudantes e professores de matemática devido à facilidade de propor problemas que podem requerer para a sua solução a utilização simultânea de métodos algébricos, analíticos, topológicos, geométricos e combinatórios, aliado à simplicidade de seus conceitos. A Teoria dos Números desperta interesse e tem a reputação de ser uma área da matemática mais significativa e que continua sendo o mais fascinante e desafiador.

Um problema importante na teoria dos números é encontrar as condições necessárias para que uma equação tenha solução em um conjunto dado. Em teoria dos números, Waring fez interessantes avanços. O problema de Waring, publicado no *Meditationes Algebraicae* em 1770, conjectura que para qualquer inteiro $k \geq 2$, existe um inteiro s dependendo somente de *k*, tal que todo inteiro positivo *n* deve ser expresso como uma soma de *s* k-ésimas potências de inteiros não negativos:

$$n = x_1^k + x_2^k + x_3^k + \ldots + x_s^k .$$

Denota-se por *g(k)* o valor mínimo *s* que se verifica a condição anterior.

Edward Waring foi um matemático inglês que, por suas realizações em matemática, recebeu uma medalha da *Royal Society Copley*. Seu principal interesse de pesquisa estava em álgebra e teoria dos números. A obra *Miscellanea Analytica*, de Edward Waring, que surgiu em 1776 e uma nova edição, ampliada em 1785, foram a base para outras obras publicadas mais tarde. *Proprietates Algebraicarum Curvarum* foram publicadas em 1772. *Meditationes Algebraicae*, que abrange a teoria de equações e a teoria dos números, bem como o que agora é conhecido como geometria analítica, surgiu em 1770, e uma versão ampliada em 1782.

Edward Waring tornou-se ainda mais conhecido devido a afirmação do problema que leva seu nome, problema de Waring: todo número natural pode se expressar como uma soma de não mais que quatro quadrados, nove cubos, dezenove quartas potências e assim por diante. Tal afirmação, sem provas, tinha apenas evidências numéricas. O problema da falta de provas para sua afirmação gerou toda uma inquietação entre os matemáticos. Muitos foram os que se sentiram motivados a provar tal afirmação.

Em 1770, o matemático francês Joseph Louis Lagrange provou que a conjectura de Waring, quando $g(2) \leq 4$, era verdade, ou seja, cada inteiro positivo é a soma quatro quadrados. Após muitas tentativas de demonstração, foi somente em 1909 que o matemático David Hilbert conseguiu demonstrar a conjectura de Waring, em que $g(k) < \infty$, para todo k. Porém, ele não determinou o valor numérico de $g(k)$ para qualquer k.

Em 1912 os matemáticos alemães Arthur Wieferich e Aubrey Kempner provaram que $g(3) \leq 9$, ou seja, cada inteiro positivo é a soma de nove cubos. Em 1964, o matemático chinês Chen Jingrun mostrou que $g(5) \leq 37$. Em 1986, três matemáticos, Ramachandran Balasubramanian da Índia e Jean-Marc Deshouillers e François Dress da França, em conjunto mostraram que $g(4) \leq 19$. Uma fórmula geral para potências mais elevadas do problema de Waring tem sido sugerida, mas não se provou ser verdadeiro para todos os inteiros.

> "Every integer is a cube or the sum of two, three, ... nine cubes; every integer is also the square of a square, or the sum of up to nineteen such; and so forth." Meditationes Algebraicæ 1770, Edward Waring.

Assim, devido a motivação criada pela conjectura de Waring, será apresentado neste trabalho como objetivo principal, o problema de Waring quando $\boldsymbol{s = k = 2}$. Apresentam-se demonstrações de condições para que se possa garantir quando um número inteiro poderá ser representado como sendo uma soma de dois quadrados, isto é, $\boldsymbol{n = x_1^2 + x_2^2}$ para $\boldsymbol{x_1, x_2}$ pertencente aos inteiros . Inclui-se o zero como um possível valor para $\boldsymbol{x_1}$ ou $\boldsymbol{x_2}$ a fim de que se possam escrever alguns quadrados como soma de dois quadrados, por exemplo, $9 = 3^2 + 0^2$.

Para melhor entendimento desta dissertação é necessário que se observe algumas definições e teoremas, a fim de que possam ser utilizadas como ferramentas.

A disposição dessa dissertação é a seguinte:

No capítulo *2*, abordar-se-á alguns assuntos relevantes tais como números inteiros não negativos, divisibilidade, máximo divisor comum e números primos.

No capítulo *3*, abordar-se-á o tema de congruência e alguns teoremas, entre eles, o pequeno teorema de Fermat, o teorema de Wilson e o teorema de Thue.

No capítulo *4*, usar-se-á as ferramentas dos capítulos *2* e *3* para se atingir o seguinte objetivo: mostrar que alguns números inteiros podem ser escritos como soma de dois quadrados, que é o principal objetivo.

No capítulo *5*, encerrar-se-á a dissertação com a conclusão do trabalho.

Encerra-se essa introdução mostrando que a elaboração desse trabalho está centrada na construção de um material de ensino envolvendo divisibilidade, máximo divisor comum, números primos e congruências e as demonstrações de que alguns números inteiros não negativos podem ser escritos como soma de dois quadrados. A tarefa de realizar a elaboração desse trabalho trouxe um grande amadurecimento do autor na área de ensino de matemática.

2 NÚMEROS PRIMOS

Os números primos, por apresentarem a característica de gerar todos os outros números sem possuir um padrão, isto é, comportando-se de maneira aleatória, causam extraordinária admiração aos matemáticos. Os números primos e suas propriedades foram estudados extensivamente pelos gregos antigos. Antes dos gregos, há alguma evidência de que os babilônios e egípcios tiveram uma compreensão de números inteiros primos através de seu sistema sexagesimal de divisão, que é um sistema de numeração posicional que usa como base aritmética o número 60. A fonte mais valiosa disponível na experiência dos antigos gregos envolvendo números inteiros primos é o extraordinário texto Elementos de Euclides. Elementos de Euclides manteve-se como sendo uma das obras de matemática mais influentes de todos os tempos. A elaboração deste livro há mais de dois mil anos, é creditado ao matemático grego Euclides. Elementos de Euclides contêm teoremas importantes sobre primos, incluindo a infinitude dos números primos e o teorema fundamental da aritmética.

2.1 DIVISIBILIDADE DE NÚMEROS INTEIROS

Representa-se por Z o conjunto dos números $\{.... -3, -2, -1, 0, 1, 2, 3,...\}$ denominados de Inteiros.

Representa-se por N o conjunto dos números {0, 1, 2, 3, ...} denominados Naturais.

Definição:

Dados dois números inteiros a e b, diz-se que **a** é divisível por b ou b é um divisor de a, representado por $b \mid a$, quando existir $c \in Z$ tal que

$$a = b.c.$$

Assim, observam-se as seguintes propriedades básicas:

i) $a \mid a, 1 \mid$ **a e a** $\mid 0$ com $a \in Z$.

ii) se $0 \mid a$, então $a = 0$ com $a \in Z$.

iii) se $a \mid 1$, então $a = \pm 1$ com $a \in Z$.

Exemplos: 2 | 6, 4 | 4, 6 | 0.

Caso ***a*** não seja divisível por ***b***, ou ***b*** não seja um divisor de ***a***, simbolicamente, escreve-se como,

$$b \nmid a.$$

Exemplos: $2 \nmid 5$, $4 \nmid 9$, $6 \nmid 13$.

Proposição 2.1.1: Se ***a***, ***b*** e ***c*** são inteiros com $c \mid b$ e $c \mid a$, então $c \mid a$.

Demonstração:

Como $b \mid a$ e $c \mid b$, então se pode representar $a = b.k$ e $b = c.q$, com ***k*** e ***q*** inteiros. Substituindo o valor de ***b*** na igualdade $a = b.k$, obtém-se:

$$a = c.q.k = c.(q.k),$$

portanto,

$$c \mid a.$$

Proposição 2.1.2: Se ***a***, ***b*** e ***c*** são inteiros com $b \mid a$, então $b.c \mid a.c$.

Demonstração:

Como $b \mid a$, então $a = b.k$, com **k** inteiro. Multiplicando ambos os lados por ***c***, obtém-se,

$$a.c = b.c.k = (b.c).k,$$

portanto, $b.c \mid a.c$, com ***c*** inteiro.

Exemplo: 6 | 12, logo 6.5 = 30 | 12.5 = 60.

Proposição 2.1.3: Se ***a***, ***b*** e ***c*** inteiros com $c \mid a$ e $c \mid b$, então $c \mid m.a \pm n.b$, para qualquer inteiro ***m*** e ***n***.

Demonstração:

Como $c \mid a$ e $c \mid b$, então se escreve $a = c.k$ e $b = c.q$, com k e q inteiros. Somando o produto da equação $a = c.k$ por m com o produto da equação $b = c.q$ por n, obtém-se:

$$a.m \pm b.n = c.(m.k) \pm c.(n.q) = c.(m.k \pm n.q),$$

portanto,

$$c \mid (m.a \pm n.b).$$

Exemplo: 3 | 21 e 3 | 33, logo 3 | (5.21+ 3.33) = 105 + 99 = 204.

3 | 21 e 3 | 33, logo 3 | (5.21 – 3.33) = 105 – 99 = 6.

2.2 MÁXIMO DIVISOR COMUM

Definição:

O máximo divisor comum de dois números inteiros a e b, com $ab \neq 0$, é o maior inteiro que divide tanto a como b, isto é,

i) $d \mid a$ e $d \mid b$;

ii) se algum $c \in N$, é tal que $c \mid a$ e $c \mid b$, então $c \leq d$.

O máximo divisor comum de a e b é representado por $d = (a, b)$.

Exemplo: (18, 32) = 2.

Dois números inteiros, a e b, cujo máximo divisor comum, (a, b), é igual a 1 são ditos primos entre si.

Exemplo: (12, 17) = 1, portanto 12 e 17 são primos ente si.

Proposição 2.2.1: Seja a, b, e c números inteiros com $(a, b) = d$. Então,

i) $(a/d, b/d) = 1$

(ii) $(a + c.b, b) = (a, b)$.

Demonstração:

i) Sejam a e b números inteiros com $(a, b) = d$. Deseja-se mostrar que 1 é o único divisor comum, positivo, de a / d e b / d. Sendo k um número inteiro positivo tal que $k \mid (a/d)$ e $k \mid (b/d)$. Assim, tem-se $(a/d) = k.r$ e $(b/d) = k.s$, com r e s inteiros. Como $a = d.k.r$ e $b = d.k.s$, então $d.k$ é um divisor comum de a e b. Como por hipótese $(a, b) = d$, conclui-se que k é igual a 1, logo $(a/d, b/d) = 1$.

ii) Sejam a, b e c números inteiros. Deseja-se mostrar que os divisores de a e b são exatamente os mesmos de $(a + c.b)$ e b. Seja $d = (a, b)$. Assim, $d \mid a$ e $d \mid b$, portanto d divide $(a + c.b)$. Sendo k, inteiro, o maior divisor comum de $(a + c.b)$ e b, tem-se que $k \mid (a + c.b - c.b) = a$. Portanto, conclui-se que $(a + cb, b) = (a, b)$.

Teorema 2.2.1: (Algoritmo da Divisão) Se $a \in Z$ e $b \in Z^+$, sempre existem e são únicos inteiros q (quociente) e r (resto) tais que $a = b.q + r$, com $0 \leq r < b$.

Demonstração:

i) Existência: Considere $q = \left[\frac{a}{b}\right]$ e $r = a - b.r$.

Sabendo que $x - 1 < [x] \leq x$, então,

$$\frac{a}{b} - 1 < \left[\frac{a}{b}\right] \leq \frac{a}{b}.$$

Multiplicando todos os termos dessa inequação por $-b$, obtém-se,

$$b - a > -b.\left[\frac{a}{b}\right] \geq -a.$$

Adiciona-se a aos três termos dessa inequação e substitui $\left[\frac{a}{b}\right]$ por q, para obter,

$$b > a - b.q \geq 0 .$$

Como $r = a - b.q$, conclui-se que $0 \leq r < b$.

ii) Unicidade: Suponha a existência de dois pares (q_1, r_1) e (q_2, r_2) em que

$$a = b.q_1 + r_1, \text{ com } 0 < r_1 \leq b \text{ e}$$
$$a = b.q_2 + r_2, \text{ com } 0 < r_2 \leq b.$$

Subtraindo as equações, obtém-se,

$$0 = a - a = (b.q_1 + r_1) - (b.q_2 + r_2) = b(q_1 - q_2) + (r_1 - r_2).$$

Daí,

$$r_1 - r_2 = b(q_1 - q_2).$$

Suponha $r_1 \neq r_2$ e $r_2 > r_1$. Então $0 < r_1 < r_2 < b$. Sabe-se que b divide $r_2 - r_1$. Então $r_1 = r_2$, o que é uma contradição. Daí $0 = b.(q_1 - q_2)$. Sendo $b > 0$ tem-se que $q_1 = q_2$.

Teorema 2.2.2: Sejam $a, b \in Z, a.b \neq 0$. Então existem $m, n \in Z$ tais que $(a, b) = m.a + n.b$.

Demonstração:

i) Pelo princípio da Boa Ordenação existe um menor número inteiro positivo d escrito como combinação linear de a e b, ou seja, $d = m.a + n.b$. Deve-se mostrar que $d \mid a$ e $d \mid b$. Pelo algoritmo da divisão tem-se que

$$a = d.q + r, \ 0 \leq r < d.$$

Substituindo d por $m.a + n.b$ na equação, tem-se,

$$a = (m.a + n.b).q + r$$

$$r = a - m.a.q - n.b.q$$

$$r = (1 - m.q).a - n.q.b$$

Observe que r é combinação linear de a e b. Más como d é o menor elemento da combinação linear de a e b e $0 \leq r < d$, pode-se concluir que $r = 0$ e que $d \mid a$. De maneira análoga pode-se demonstrar que $d \mid b$.

ii) Agora, será mostrado que d é o maior divisor comum de a e b. Para mostrar isso, deve-se mostrar que qualquer divisor comum c de a e b deve dividir d. Sendo $d = ma + nb$ e por hipótese $c \mid a$ e $c \mid b$, então se conclui que $c \mid (m.a + m.b) = d$.

2.3 NÚMEROS PRIMOS

2.3.1.Definição:

Um número inteiro positivo p é chamado número primo (ou simplesmente primo), se p possui como divisores exatamente dois divisores positivos que são: o 1 e p (*ele mesmo*).

Exemplos: ***2, 3, 5, 7, ...*** são números primos.

Um número maior que 1 e que possua mais de dois divisores positivos é denominado de número composto. São exemplos de números compostos: ***4, 6, 8, 9, ...*** .

Proposição 2.3.1. Todo número inteiro maior do que 1 possui um divisor primo.

Demonstração:

Supõe-se que exista um número inteiro maior que 1 e que não possua divisores primos. Uma vez que o conjunto formado pelos números maiores que 1, inteiros, sem divisores primos não é vazio, então pelo princípio da Boa Ordenação, existe um menor número inteiro positivo n maior que 1 e que não possui divisores primos. Como n não possui divisores primos e n divide n, então n não é um número primo. Daí pode-se escrever:

$$n = a.b, \text{ com } 1 < a < n \text{ e } 1 < b < n.$$

Como $a < n$, a terá um divisor primo. Como qualquer divisor de a, é também divisor de n, temos uma contradição, pois n não possui nenhum divisor primo. Logo se pode concluir que todo número inteiro positivo tem pelo menos um divisor primo.

Exemplos: n = 7 = 1.7. Possui um divisor primo, que é o 7.

n = 30 = 1.2.3.5. Possui três divisores primos, que são: 2, 3 e 5.

Euclides foi um matemático, nascido provavelmente na Grécia, muitas vezes, referido como o "Pai da Geometria". Ele é até hoje, na história da matemática, considerado como um dos mais significativos estudiosos da geometria. Fez parte do quadro de professores da recém-fundada Escola Real de Alexandria a convite de Ptolomeu I que governou o Egito de 323 a.C a 283 a.C. Pelos métodos utilizados em suas aulas de geometria e álgebra tornou-se bastante influente. Escreveu uma das obras matemáticas mais permanentes de todos os tempos, conhecido como o 'Elementos' que compreendem 13 volumes gigantescos cheios de teorias e conhecimentos geométricos. Seu livro Elementos é uma das obras mais influentes da história da matemática, que serve como o principal livro didático de matemática especialmente a parte da geometria. Euclides também escreveu obras em perspectiva, cônicas, geometria esférica e teoria dos números.

Agora será demonstrado o ***Teorema 2.3.1.*** em que Euclides afirma que existem infinitos números primos, porém pode-se perceber que este teorema não mostra que todos os números obtidos são números primos, mas que existe entre eles uma quantidade infinita de números primos.

Teorema 2.3.1. (*Teorema de Euclides*). Existem infinitos números primos.

Demonstração:

Supõe-se que exista uma quantidade finita de números primos, $p_1, p_2, p_3, ..., p_k$. Multiplicando os números primos $p_1, p_2, p_3, ..., p_k$ e adicionando 1, obtém-se um novo número natural diferente de $p_1, p_2, p_3, ..., p_k$. Pela ***Proposição 2.3.1***, existe um número primo q que é divisor de N e por suposição $q = p_i$, para algum $i, 1 \leq i \leq k$. Tem-se que q divide N como também q divide $N - 1 = p_1. p_2. p_3. .....p_k$, portanto pela ***Proposição 2.1.3***, $q \mid N - (N -$

1) = 1, o que é uma contradição, pois todo número primo é maior que ***1*** e, consequentemente, não divide ***1***. Logo, ***q*** não pode estar no conjunto finito de primos, $p_1, p_2, p_3, ..., p_k$. Isso significa que pelo menos mais um número primo existe além dos que estão no conjunto $p_1, p_2, p_3, ..., p_k$,. Isso prova que para qualquer conjunto finito de números primos, há um número primo que não está nesse conjunto. Portanto, existem infinitos números primos.

Exemplo: 2.3.5.7 + 1 = 211 é primo.

2.3.5.7.11.13 + 1 = 30031 = 59.509, portanto 30031 não é primo.

Proposição 2.3.2. Se ***p*** é primo e $x_1, x_2, x_3, ..., x_n$ são alguns números inteiros tal que $p \mid x_1.x_2.x_3 ..... x_n$, então $p \mid x_i$ para algum x_i $(1 \leq i \leq n)$.

Demonstração:

i) Esta demonstração será feita utilizando o princípio da indução finita. O resultado é inteiramente verdadeiro para quando ***n = 1***, porém para uma melhor compreensão, é conveniente começar por provar o caso para quando ***n = 2***. Supõe-se então que $p \mid x_1.x_2$. Deve-se provar que, se ***p*** não divide x_1 então ***p*** deve dividir x_2. Agora, se ***p*** não divide x_1 então como ***1*** e ***p*** são os únicos divisores positivos de ***p***, deve-se ter $mdc(p, x_1) = 1$. Portanto, existem ***r*** e ***s*** números inteiros tais que $r.p + s.x_1 = 1$. Assim

$$x_2 = 1.x_2 = (r.p + s.x_1).x_2 = (r.x_2).p + s.(x_1\ x_2).$$

Como ***p*** divide ambas as parcelas, $(r.x_2).p$ e $s.(x_1\ x_2)$, segue-se que ***p*** divide x_2.

ii) Supondo que o resultado vale para quando ***n = k***, deve-se provar o caso ***n = k + 1***. Se $p \mid x_1.x_2. . . x_k.x_{k+1}$, então $p \mid X.x_{k+1}$ onde $X = x_1.x_2.x_3 ..... x_n$. Se $p \mid X$ então, pela hipótese de indução, $p \mid x_i$ para alguns x_i no intervalo $1 \leq i \leq k$. Por outro lado, se ***p*** não divide ***X***, então deve se ter que $p \mid x_{k+1}$, usando o resultado para o caso quando ***n = 2***. Assim, pelo princípio da indução finita, pode-se concluir que o resultado é válido para todo valor de ***n***.

Proposição 2.3.3. Existe uma infinidade de números primos da forma ***4m + 3***.

Demonstração:

Suponha que exista uma quantidade finita de números primos da forma $4m + 3$, $p_0 = 3, p_1, p_2, p_3, ..., p_k$. Fazendo $N = 4(p_1. p_2. p_3. .... p_k) - 1 = 4(p_1. p_2. p_3. .... p_k - 1) + 3$. Assim, existe pelo menos um número primo na fatoração de N escrito da forma $4m + 3$. Caso contrário, todos esses números primos seriam escritos da forma $4m + 1$, e como o produto de dois termos escritos da forma $4m + 1$ também é escrito da forma $4m + 1$, ou seja,

$$(4r + 1).(4s + 1) = 16rs + 4r + 4s + 1 = 4(4rs + r + s) + 1,$$

isso implicaria que N também seria dessa forma, o que é uma contradição. No entanto, nenhum dos primos, $p_0, p_1, p_2, p_3, ..., p_k$ divide N. O número primo 3 não divide N, pois se $3 \mid N$, então $3 \mid (N - 3) = 4(p_1 p_2 ... p_k - 1)$, o que é uma contradição. Da mesma forma, nenhum dos primos pj, $1 \leq j \leq k$, pode dividir N, porque se $pj \mid N$ implicaria em $pj \mid [N - 4(.p_1. p_2. p_3. ... p_k - 1)] = 3$, que é uma contradição. Assim, existem infinitos números primos da forma $4m + 3$.

Exemplos: Seja $p_1 = 3$ e $p_2 = 7$. Então $N = 4(3.7 - 1) + 3 = 83$ é primo e da forma $4m + 3$ quando $m = 20$.

Seja $p_1 = 3$, $p_2 = 7$ e $p_3 = 83$. Então $N = 4(3.7.83 - 1) + 3 = 6971$ é primo e da forma $4m + 3$ quando $m = 1742$.

O teorema fundamental da aritmética é um resultado importante, pois mostra que os números primos são a base da construção dos números inteiros e garante a obtenção de uma representação única para todo e qualquer número inteiro positivo. Isso abre diversas possibilidades de aplicação, como na criptografia.

Teorema 2.3.2. (*Teorema Fundamental da Aritmética*). Todo número inteiro maior que 1 ou é primo ou pode ser representado de maneira única, a menos da ordem dos fatores, como um produto de fatores primos.

Demonstração:

i) De início, será mostrado que cada número inteiro positivo pode ser escrito como o produto de números primos. Usa-se a contradição para essa demonstração. Suponha que exista algum número inteiro positivo, $n \in N, n > 1$, que não possa ser escrito como um produto de fatores primos e que não seja primo. Usando o princípio da Boa Ordenação, existe um menor número inteiro positivo, denominado de $n_1 > 1$ que não pode ser escrito como um produto de números primos, nem pode ser primo. O número n_1 não pode ser um número primo porque, caso contrário, ele seria o próprio fator da fatoração e por hipótese n_1 não pode ser fatorado em primos. Isso significa dizer que n_1 possui alguns divisores entre 1 e n_1. Daí pode-se escrever $n_1 = a.b$ para alguns números inteiros a e b, em que $1 < a < n_1$ e, por conseguinte, $1 < b < n_1$. Uma vez que n_1 é o menor número que não pode ser fatorado em primos e a e b são menores, então a e b devem possuir primos em sua fatoração. Assim, pode-se escrever $a = p_1.p_2 \cdot \cdot \cdot p_r$ e $b = q_1.q_2 \cdot \cdot \cdot q_s$ para alguns primos p_i e q_j. Mas isso significa dizer que $n_1 = a.b = p_1.p_2 \cdot \cdot \cdot \cdot \cdot \cdot p_r.q_1. q_2 \cdot \cdot \cdot q_s$, ou seja, n_1 é um produto de números primos, que é uma contradição. Portanto, a hipótese assumida ao início está equivocada. Logo, todos os números inteiros, $n \in N, n > 1$ podem ser escritos como um produto de números primos ou são primos.

ii) Agora, será mostrada a unicidade. Sendo $n \in N, n > 1$ e assumindo que $n = p_1.p_2 \cdot \cdot \cdot p_r$ e $n = q_1.q_2 \cdot \cdot \cdot q_s$ em que os p_i $(1 < i < r)$ são números primos, não necessariamente distintos e os q_j $(1 < j < s)$ são números primos, não necessariamente distintos, deve-se mostrar, portanto, que essas fatorações devem ser as mesmas, isto é, são iguais. Uma vez que ambas as fatorações são iguais a n, temos $p_1.p_2 \cdot \cdot \cdot p_r = n = q_1.q_2 \cdot \cdot \cdot q_s$. Supõe-se que as fatorações sejam diferentes. Depois de cancelar todos os fatores comuns de ambos os lados, alguns números primos, diferentes, irão permanecer em cada lado (caso isso não acontecesse as fatorações seriam iguais). Tem-se que $p_1 | n$, então $p_1 | q_1.q_2 \cdot \cdot \cdot q_s$. Como p_1 é primo, então p_1 divide um dos fatores de $n = q_1.q_2 \cdot \cdot \cdot q_s$, denominado de q_j para algum j. Sendo q_j primo e $p_1 > 1$, então se pode dizer que $p_1 = q_j$. De acordo com a situação, podem-se reorganizar os q_j, para que se tenha $p_1 = q_1$. Cancelando p_1 com q_1 na equação $p_1.p_2 \cdot \cdot \cdot p_r = n = q_1.q_2 \cdot \cdot \cdot q_s$, obtém-se $p_2 \cdot \cdot \cdot p_r = q_2 \cdot \cdot \cdot q_s$. Mas $p_2 \cdot \cdot \cdot p_r < n$ e assumindo que n é o menor inteiro positivo, tem-se que $r = s$ e assim se pode deduzir que os fatores $p_2 \cdot \cdot \cdot p_r$ são os mesmos que $q_2 \cdot \cdot \cdot q_s$ em uma certa ordem. Isso é uma contradição, pois por suposição as fatorações $n = p_1.p_2 \cdot \cdot \cdot p_r$ e $n = q_1.q_2 \cdot \cdot \cdot q_s$ eram fatorações diferentes. Assim, pode-se concluir que não pode existir um mesmo número com duas fatorações diferentes. Dessa forma, fica provada a unicidade.

Existe a possibilidade de se ter alguns números primos repetidos na fatoração de um número composto. Nesse caso, podem-se agrupar os números primos iguais usando a potenciação, ou seja, todo número inteiro n pode ser escrito da forma:

$$n = p_1^{\alpha_1} . p_2^{\alpha_2} . p_3^{\alpha_3} ..... p_s^{\alpha_s} ,$$

em que todos os p_i são números primos distintos e os α_i são números maiores ou iguais a 1 com $1 \leq i \leq s$.

Exemplo: 36 pode ser escrito como sendo 6.6, ou 4.9, ou 3.12, ou 2.18. Mas só há uma maneira de escrevê-lo como um produto em que todos os fatores são primos:
$36 = 2.2.3.3 = 2^2.3^2$

3 CONGRUÊNCIA

3.1 DEFINIÇÃO:

Se a e b e m são números inteiros e $m > 0$, cuja diferença é divisível por m (escreve-se: $m \mid (a - b)$), diz-se que a é congruente a b módulo m,

$$a \equiv b \bmod m;$$

Esta notação especial, segundo Gauss tem a vantagem de envolver apenas as quantidades que são essenciais para a ideia envolvida, ao passo que na expressão $a = b + cm$, existe um fator c que é irrelevante. Essa notação de Gauss é de grande importância e conveniência no estudo da teoria de divisibilidade.

Exemplo: $38 \equiv 2 \bmod 4$, pois $4 \mid (38 - 2)$. Da mesma forma que $3 \equiv -1 \bmod 4$ e $187 \equiv 3 \bmod 4$.

Se $m \nmid (a - b)$ então a não é congruente a b módulo m e escreve-se

$$a \not\equiv b \bmod m.$$

Exemplo: $75 \not\equiv 5 \bmod 4$.

Apresentam-se agora algumas das propriedades de congruência módulo m.

Proposição 3.1.1. Congruência módulo **m** é uma relação de equivalência.

i) Reflexiva: $a \equiv a \bmod m$, para qualquer número inteiro a.

ii) Simetria: Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$, quaisquer que sejam a, b inteiros.

iii) Transitiva: Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$, quaisquer que sejam a, b, c inteiros.

Demonstrações:

i) Observe que m divide $0 = a - a$, portanto $a \equiv a \bmod m$.

Exemplos: $5 \equiv 5 \bmod 2$, $7 \equiv 7 \bmod 3$.

ii) Observe que m divide $a - b$, então m também divide $-(a - b) = b - a$, portanto $b \equiv a \bmod m$.

Exemplo: $15 \equiv 11 \bmod 2$, logo $11 \equiv 15 \bmod 2$.

iii) Observe, por hipótese, que m divide $a - b$ e divide $b - c$, então m também divide $(a - b) + (b - c) = a - c$, portanto $a \equiv c \bmod m$.

Exemplo: $15 \equiv 7 \bmod 4$ e $7 \equiv 3 \bmod 4$, logo $15 \equiv 3 \bmod 4$.

Proposição 3.1.2. Congruências podem ser adicionadas, multiplicadas e elevadas a uma determinada potência.

i) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$, quaisquer que sejam a, b, c e d inteiros.

ii) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a.c \equiv b.d \bmod m$, quaisquer que sejam a, b, c e d inteiros.

iii) Se $a \equiv b \bmod m$, então $ak \equiv bk \bmod m$ onde k inteiro não negativo, quaisquer que sejam a e b inteiros.

iv) Se a, b, k e m são inteiros tal que $k > 0$, $m > 0$, e $a \equiv b \bmod m$, então $a^k \equiv b^k \bmod m$.

Demonstrações:

i) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a = b + mt$ e $c = d + mn$. Somando membro a membro as duas últimas igualdades, tem-se:

$$a + c = b + mt + d + mn$$

$$a + c = (b + d) + (t + n)m.$$

Portanto,

$$a + c \equiv b + d \bmod m.$$

Exemplo: 5 ≡ 2 mod 3 e 7 ≡ 1 mod 3, logo 12 ≡ 3 mod 3, isto é, 5 + 7 ≡ 2 + 1 mod 3.

ii) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a = b + mt$ e $c = d + mn$. Multiplicando-se membro a membro as duas últimas igualdades, tem-se:

$$ac = (b + mt)(d + mn)$$

$$ac = bd + bmn + dmt + m^2tn$$

$$ac = bd + (bn + dt + mtn)m.$$

Portanto,

$$ac \equiv bd \bmod m.$$

Exemplo: 5 ≡ 2 mod 3 e 7 ≡ 1 mod 3, logo 35 ≡ 2 mod 3, isto é, 5.7 ≡ 2.1 mod 3.

iii) Se $a \equiv b \bmod m$, então $a = b + mt$. Multipicando a por k, obtém-se:

$$ak = k(b + mt)$$

$$ak = kb + kmt$$

$$ak \equiv bk \bmod m.$$

Exemplo: 7 ≡ 1 mod 3, logo 14 ≡ 2 mod 3, isto é, 7.2 ≡ 1.2 mod 3

iv) Se $a \equiv b \bmod m$, então $m \mid a - b$. Sabe-se que

$$a^k - b^k = (a-b)\left(a^{k-1} + a^{k-2}.b + \ldots\ldots + a.b^{k-2} + b^{k-1}\right).$$

Pode-se perceber que $(a-b) \mid a^k - b^k$ e como $m \mid (a-b)$, pela propriedade transitiva, tem-se que,

$$m \mid a^k - b^k .$$

Logo,

$$a^k \equiv b^k \bmod m.$$

Exemplo: $5 \equiv 2 \bmod 3$, logo $3 \mid (5-2)$. Fazendo $609 = 5^4 - 2^4 = (5-2).(5^3 + 5^2.2 + 5.2^2 + 2^3)$, pode-se notar que $(5-2) \mid (5^4 - 2^4)$. Pela propriedade transitiva $3 \mid (5^4 - 2^4)$. Logo, pode-se concluir que $5^4 \equiv 2^4 \bmod 3$.

Agora, serão apresentados os ***Lemas*** (***3.1*** e ***3.2***) necessários para a demonstração e melhor entendimento do teorema de Wilson.

Lema 3.1: Seja p primo. O inteiro positivo é a sua própria inversa módulo p se e somente se $a \equiv 1 \bmod p$ ou $a \equiv -1 \bmod p$.

Demonstração:

Se $a \equiv 1 \bmod p$ ou $a \equiv -1 \bmod p$, então $a^2 \equiv 1 \bmod p$, de modo que a é o seu próprio inverso módulo p. Inversamente, se a é o seu próprio inverso, então $a^2 = a.a \equiv 1 \bmod p$. Assim $p \mid (a^2 - 1)$, ou seja $p \mid (a+1).(a-1)$. Logo $p \mid (a+1)$ ou $p \mid (a-1)$ e pode ser expresso da seguinte forma:

$$a - 1 \equiv 0 \bmod p \quad \text{ou} \quad a + 1 \equiv 0 \bmod p.$$

Portanto,

$$a \equiv 1 \bmod p \text{ ou } a \equiv -1 \bmod p.$$

Lema 3.2: Seja p um número primo ímpar, e seja a_1 uma solução da equação $a.x \equiv 1 \bmod p$, $a = 1.2.3....(p-1)$, onde $a.a_1 \equiv 1 \bmod p$ e $0 \leq a_1 < p$. Então $a_1 \not\equiv b_1 \bmod p$ se $a \not\equiv b \bmod p$, e $a_1 \equiv a \bmod p$ somente quando $a = 1$ ou $a = p - 1$.

Demonstração:

Pode-se observar que $mdc(a, p) = 1$ e que a_1 pode ser determinado e é único, pois a equação $a.x \equiv 1 \bmod p$ tem exatamente uma única solução. Supondo-se que $a_1 \equiv b_1 \bmod p$, então multiplicando ambos os termos por a, obtém-se:

$$a.a_1 \equiv ab_1 \bmod p.$$

Substituindo $a.a_1$ por 1, obtém-se

$$1 \equiv ab_1 \bmod p.$$

Multiplicando ambos os termos por b, obtém-se

$$b \equiv a.b_1.b \bmod p.$$

Substituindo $b_1.b$ por 1, obtém-se,

$$b \equiv a \bmod p.$$

Supondo-se agora que $a \equiv a_1 \bmod p$. Multiplicando ambos os termos por a, obtém-se:

$$1 \equiv a.a_1 \equiv a^2 \bmod p,$$

Portanto do ***Lema 3.2***, pode-se concluir que $a = 1$ ou $a = p - 1$.

Exemplo: Fazendo p = 11, tem-se:

a	≡	**1**,	**2**,	**3**,	**4**,	**5**,	**6**,	**7**,	**8**,	**9**,	**10** mod **11**
a_1	≡	**1**,	**6**,	**4**,	**3**,	**9**,	**2**,	**8**,	**7**,	**5**,	**10** mod **11**
$a.a_1$	≡	**1**,	**12**,	**12**,	**12**,	**45**,	**12**,	**56**,	**56**,	**45**,	**100** mod **11**

Observa-se que os números que se encontram na segunda linha são os mesmos da primeira, porém em outra ordem, que $a.a_1 \equiv 1 \bmod 11$ em todos os termos e $a \equiv a_1 \bmod 11$ quando $a = 1$ ou $a = 11 - 1 = 10$.

3.2 TEOREMA DE WILSON.

John Wilson era inglês, matemático. Estudou em Staveley, Cumbria antes de ir até Peterhouse, Cambridge em 1757, onde foi aluno de Edward Waring. Seu nome está associado ao teorema na teoria dos números, publicado por Edward Waring em sua obra Meditationes Algebraicae.

***Teorema 3.2.1*:** Se p é primo, então $(p-1)! \equiv -1 \bmod p$.

Demonstração:

Observe que $(2-1)! \equiv -1 \bmod 2$. Assim, o teorema é verdadeiro para $p = 2$. Atribuindo a p, primo, um valor maior que 2, tem-se que, usando o ***Lema 3.2***, para cada inteiro a com $1 \leq a \leq p-1$, existe um inverso a_1, $1 \leq a_1 \leq p-1$, com $a.a_1 \equiv 1 \bmod p$. Do ***Lema 3.1***, os únicos números inteiros positivos menores que p que são seus próprios inversos são 1 e $p-1$. Retirando os termos 1 e $p-1$, fica-se com os $p-3$ termos restantes:

$$2, 3, 4, \ldots\ldots, p-3, p-2$$

Podem-se separar os termos em $\frac{(p-3)}{2}$ pares de tal modo que cada par é constituído por um número inteiro a e a ele associado um número inteiro a_1, que é diferente de a. O produto desses dois números inteiros em cada par $(a.a_1)$ é congruente a $1 \bmod p$. Daí, tem-se que:

$$2.3.4\ldots\ldots(p-3).(p-2) \equiv 1 \bmod p.$$

Multiplicando ambos os membros por 1 e $p-1$, obtém-se:

$$1.2.3.4\ldots\ldots(p-2).(p-1) \equiv 1.(p-1) \bmod p$$

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

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

Exemplo: Fazendo p = 7. Tem-se que (7 – 1) ! = 6 ! = 1.2.3.4.5.6. Reorganizando os fatores presentes na multiplicação e agrupando os pares de inversos módulo 7, observa-se que $2.4 \equiv 1 \bmod 7$ e $3.5 \equiv 1 \bmod 7$. Consequentemente $6\,! = 1.(2.4).(3.5).6 \equiv 1.6 \equiv -1 \bmod 7$.

Uma observação bastante interessante e que nos fornece um método para determinar primos é que a recíproca do teorema de Wilson também é verdade, como mostra o seguinte teorema.

Teorema 3.2.2: Se p é um número inteiro positivo, tal que $(p-1)\,! \equiv -1 \bmod p$, então p é primo.

Demonstração:

Suponha p um número inteiro composto e que $(p-1)\,! \equiv -1 \bmod p$. Sendo p um número composto, então, pode-se escrevê-lo como sendo $p = a.b$, onde $1 < a < p$ e $1 < b < p$. Como $(p-1)\,! \equiv -1 \bmod p$, então, pode-se afirmar que

$$p \mid (p-1)\,! + 1$$

e como $a \mid p$, então

$$a \mid [(p-1)\,! + 1].$$

Mas como $a \leq p - 1$, segue-se que um dos fatores de $(p-1)\,!$ é ele mesmo. Assim

$$a \mid (p-1)\,!.$$

Como

$$a \mid [(p-1)\,! + 1] \text{ e } a \mid (p-1)\,!,$$

pode-se concluir que

$$a \mid [(p-1)\,! + 1 - (p-1)\,!]$$

$$a \mid 1.$$

Isso é uma contradição, pois $a > 1$. Assim, os únicos divisores positivos de p são 1 e p, e sendo assim, p é primo.

Exemplo: Fazendo p = 6. Tem-se que (6 – 1) ! = 5 ! = 120 ≡ 0 mod 6. Pelo ***Teorema 3.2.2*** observa-se que 6 não é primo.

3.3 PEQUENO TEOREMA DE FERMAT

Fermat era francês, matemático e advogado. Deixou grandes contribuições na matemática nas áreas da geometria analítica, probabilidade entre outras. Foi na teoria dos números que ocorreu um dos mais importantes legados deixado por Fermat. Foi enquanto pesquisava números perfeitos (um número é dito perfeito se for igual à soma de seus divisores próprios. Denominam-se divisores próprios de um número positivo N todos os divisores inteiros positivos de N exceto o próprio N. Por exemplo: o número 6 possui como divisores próprios os números 1, 2 e 3, cuja soma é igual à 6) que ele descobriu o teorema, denominado o pequeno teorema de Fermat.

Teorema 3.3.1: Se p é primo e a é um número inteiro positivo tal que p não divide a, então,

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

Demonstração:

Considere o conjunto $\{a, 2.a, 3.a, \ldots, (p-1).a\}$ com $p - 1$ números inteiros. Nenhum desses números inteiros são divisíveis por p, pois se p divide $j.a$, então p divide j, uma vez que por hipótese p não divide a. Isso é incoerente, pois $1 \leq j \leq p - 1$. Além disso, $a, 2a, \ldots, (p-1)a$ são incongruentes entre si módulo p. É fácil mostrar que, assumindo $j.a \equiv k.a \bmod p$, pode-se obter como conclusão que $j \equiv k \bmod p$, já que o $mdc(a, p) = 1$. Isso é impossível, uma vez que j e k são números inteiros menores que $p - 1$. Sendo os números inteiros $a, 2.a, \ldots, (p-1).a$ os elementos do conjunto de $p - 1$ números inteiros com todos incongruentes a zero e não existindo qualquer dois congruentes entre si $\bmod p$, então $a, 2.a, \ldots$

, (p – 1).a são congruentes, em alguma ordem aos ***1, 2, ... , p – 1***. Assim, o produto de todos os números inteiros ***a, 2.a, ... , (p – 1.).a*** é congruente ao produto dos ***p – 1*** números inteiros ***mod p***. Pode-se concluir, então, que

$$a.2.a.3.a.....(p-1).a \equiv 1.2.3.....(p-1) \ mod\ p$$

$$a^{p-1}.1.2.3.....(p-1) \equiv 1.2.3.....(p-1) \ mod\ p$$

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

Como o ***mdc(p, (p – 1)!) = 1***, pode-se cancelar o fator ***(p – 1)!*** e obtém-se o que se queria demonstrar,

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

3.4 TEOREMA DE THUE

Alex Thue foi um matemático, norueguês, conhecido por seu trabalho original em aproximação diofantina e combinatória. Thue foi honrado por ter sido eleito para a Academia Norueguesa de Ciências e Letras em 1894 e para o Real da Noruega Sociedade de Ciências, em Trondheim, 1895. Ele serviu como um editor de Acta Mathematica de 1916 a 1922.

Teorema 3.4.1: Seja ***p*** um número inteiro positivo. Para qualquer número inteiro ***a*** tal que ***p*** ł ***a***, existe ***x***, ***y*** $\in$ ***{1, 2, 3, ..., $\lfloor\sqrt{p}\rfloor$ }*** tal que ***a.x ≡ y mod p*** ou ***a.x ≡ – y mod p***.

Demonstração:

Para ***p = 1***, o teorema torna-se verdadeiro, pois, neste caso, tem-se ***x = y = 1.*** Supondo agora que ***p*** seja um número natural maior que ***1***. Seja ***q*** um número natural menor ou igual a $\sqrt{p}$. Então

$$q + 1 > \sqrt{p} \text{ e assim } (q+1)^2 > p.$$

Consideram-se todas as expressões da forma ***a.x – y***, para ***x*** e ***y*** assumindo os valores ***{0, 1, 2, ... , q}***. Pode-se observar que existem $(q+1)^2 > p$ números e que existem apenas ***p*** restos

possíveis ao dividir um número por p, portanto pelo princípio da casa dos pombos, irão existir pelo menos dois desses números escritos da forma $a.x - y$ que são congruentes módulo p. Tomando dois pares diferentes, ou seja, $(x_1, y_1) \neq (x_2, y_2)$ tal que $a.x_1 - y_1 \equiv a.x_2 - y_2 \bmod p$. Reorganizando a congruência, obtém-se $a.(x_1 - x_2) \equiv y_1 - y_2 \bmod p$. Fazendo $x = |x_1 - x_2|$ e $y = |y_1 - y_2|$. Excluir-se-á a possibilidade de $x = 0$ ou $y = 0$, de modo que $x, y \in \{1, 2, 3, ..., \lfloor\sqrt{p}\rfloor\}$.

i) supondo-se que $x = |x_1 - x_2| = 0$, então se pode concluir que $x_1 = x_2$. Logo $a.(x_1 - x_2) = 0 \equiv y_1 - y_2 \bmod p$. Uma vez que $y_1, y_2 \in \{0, 1, 2, 3, ..., \lfloor\sqrt{p}\rfloor\}$ sabe-se que $y_1 < p$ e que $y_2 < p$. Então obtém-se $y_1 = y_2$ e, consequentemente, chega-se a uma contradição, pois $(x_1, y_1) \neq (x_2, y_2)$.

ii) supondo-se agora que $y = |y_1 - y_2| = 0$, então $y_1 = y_2$. Assim $a.(x_1 - x_2) \equiv 0 = y_1 - y_2 \bmod p$. Como por hipótese p ł a, tem-se $x_1 - x_2 \equiv 0 \bmod p$. Então se obtém $x_1 = x_2$, e, consequentemente, chega-se a uma contradição, pois $(x_1, y_1) \neq (x_2, y_2)$. Assim, $x_1 - x_2 \neq 0$ e $y_1 - y_2 \neq 0$. Pode-se supor, sem perda de generalidade, que $x_1 - x_2 > 0$ e, neste caso, toma-se $x = x_1 - x_2$ e $y = |y_1 - y_2|$. Logo, conclui-se que $a.x \equiv y \bmod p$ ou $a.x \equiv -y \bmod p$, conforme se queria demonstrar.

Exemplo: Fazendo p = 29 e a = 17, inteiros primos entre si, em que p ł a, tem-se $17x \equiv y \bmod 29$. Como $0 < |x_1| < \sqrt{29}$ e $0 < |y_1| < \sqrt{29}$ então se tem $x, y \in \{1, 2, 3, 4, 5\}$. Testando os valores obtém-se x = 2 e y = 5.

4 NÚMEROS INTEIROS QUE PODEM SER ESCRITOS COMO SOMA DE DOIS QUADRADOS.

Muitos são os que acreditam que os números inteiros foram um dos primeiros sistemas numéricos desenvolvidos para a contagem, mas isso não é verdade, já que os nossos antepassados usaram seus dedos ou objetos como “pequenas pedras” para contar. A história dos Inteiros existe desde os tempos da Babilônia, há cerca de 4000 anos. A evolução dos números, assim como a dos conjuntos numéricos, surgiu de modo a contribuir com a necessidade da humanidade em contar. Sabe-se que o conjunto dos números inteiros são números não fracionários e que podem ser representados pelos números negativos, zero ou positivos. Os números inteiros apareceram quando os números naturais não conseguiam mais satisfazer todas as necessidades, como, por exemplo, para suprir a inexistência de números negativos no conjunto dos naturais. O conjunto dos números inteiros não negativos tinha como finalidade contar objetos, animais, enfim, elementos do contexto histórico no qual se encontravam. Sua importância é indiscutível. Os números inteiros estão presentes até hoje em diversas situações do cotidiano da humanidade, como, por exemplo, para medir temperaturas, contar dinheiro, marcar as horas etc. Diante disso, será estudado neste capítulo mais uma situação relativa aos números inteiros que é descrever condições de expressar alguns números inteiros como soma de dois quadrados.

Observe as seguintes igualdades:

$0 = 0^2 + 0^2$ $\qquad$ $5 = 2^2 + 1^2$

$1 = 1^2 + 0^2$ $\qquad$ $8 = 2^2 + 2^2$

$2 = 1^2 + 1^2$ $\qquad$ $9 = 3^2 + 0^2$

$4 = 2^2 + 2^2$ $\qquad$ $10 = 3^2 + 1^2$

Examinando as igualdades expostas acima, pode-se observar que não são todos os número inteiros que podem ser escritos como soma de dois quadrados. Neste capítulo será mostrado quais as condições para que um número inteiro possa ser escrito como soma de dois quadrados.

***Proposição 4.1*:** Se p pertence a N e é da forma $p = 4m + 3$, então não existem números inteiros x e y tais que $p = x^2 + y^2$.

Demonstração:

Dado $a \in Z$, $a \equiv 0, 1, 2 \text{ ou } 3 \bmod 4$ e $a^2 \equiv 0$ *ou* $1 \bmod 4$. Substituindo a por x e y, tem-se que $x^2 \equiv 0$ ou $1 \bmod 4$ e $y^2 \equiv 0$ ou $1 \bmod 4$. Logo $x^2 + y^2$ é congruente a $0,1$ ou $2 \bmod 4$. Então não pode-se ter $x^2 + y^2 \equiv 3 \bmod 4$, isto é $x^2 + y^2 \neq 4m + 3$ qualquer que seja m.

Exemplo: 203 ≡ 3 mod 4. Como 203 é da forma 4m + 3, então, o número 203 não pode ser escrito como soma de dois quadrados.

Teorema 4.1. *(Teorema de Fermat para dois quadrados)*: Um número primo p é escrito como soma de dois quadrados se, e somente se, $p = 2$ ou $p \equiv 1 \pmod 4$.

Demonstração:

i) Obviamente que $p = 2$ pode ser escrito como soma de dois quadrados, pois $2 = 1^2 + 1^2$.

ii) Suponha que $p > 2$ e $p = 4m + 1$, ou seja, $p \equiv 1 \bmod 4$, também pode-se escrevê-lo como soma de dois quadrados. De acordo com as igualdades acima, pode-se perceber que para todo número primo ímpar, p é congruente a 1 módulo 4 $(p \equiv 1 \bmod 4)$ ou então p é congruente a 3 módulo 4 $(p \equiv 3 \bmod 4)$. Como para qualquer que seja o valor de a inteiro, vale que $a^2 \equiv 0$ ou $1 \bmod 4$, então conclui-se: $0^2 \equiv 0 \bmod 4$, $1^2 \equiv 1 \bmod 4$, $2^2 = 4 \equiv 0 \bmod 4$, $3^2 = 9 \equiv 1 \bmod 4$. Agora, considere $p = x^2 + y^2 \bmod 4$. Como x^2 é congruente a $0 \bmod 4$ ou $1 \bmod 4$ e y^2 é congruente a $0 \bmod 4$ ou $1 \bmod 4$, pode-se perceber que $p = x^2 + y^2$ é congruente a $0, 1$ ou 2 módulo 4; no entanto como p é um número primo e maior que 2, conclui-se que p é um número impar. Logo $p \equiv 1 \bmod 4$.

iii) Supondo $p \equiv 1 \bmod 4$. Deve-se mostrar que se $a^2 + 1 \equiv 0 \bmod p$ tem solução para algum a, então p pode ser representado como soma de dois quadrados. Para isso. em primeiro lugar, deve-se analisar os fatores em $(p - 1)!$:

$$(p - 1)! = (p - 1).(p - 2). \ldots\ldots 2.1.$$

Como p é um número primo e impar, tem-se um número par de termos em que os elementos centrais serão: $\frac{(p-1)}{2}$ e $\frac{(p+1)}{2}$. Portanto,

$$(p-1)! = (p-1).(p-2).....\frac{(p+1)}{2}.\frac{(p-1)}{2}.....2.1.$$

Observe que

$$(p-1) \equiv -1 \bmod p,\ (p-2) \equiv -2 \bmod p\ ,.....\ ,\ \frac{(p+1)}{2} \equiv -\frac{(p-1)}{2} \bmod p.$$

Substituindo em $(p-1)!$ as congruências acima, obtém-se:

$$(p-1)! = (-1).(-2).....\left(-\frac{(p-1)}{2}\right).\frac{(p-1)}{2}.....2.1 \bmod p$$

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

$$(p-1)! = (-1)^{\frac{(p-1)}{2}}.\left(1.2.....\left(\frac{(p-1)}{2}\right)\right)^2 \bmod p.$$

Segundo o Teorema de Wilson (***Teorema 3.2.1***), $(p-1)! \equiv -1 \bmod p$, portanto

$$-1 \equiv (-1)^{\frac{(p-1)}{2}}.\left(1.2.....\left(\frac{(p-1)}{2}\right)\right)^2 \bmod p\ .$$

Multiplicando ambos os membros da igualdade por $(-1)^{\frac{(p-1)}{2}}$, obtém-se:

$$(-1)^{\frac{(p+1)}{2}} \equiv \left((-1)^{\frac{(p-1)}{2}}\right)^2.\left(1.2.....\left(\frac{(p-1)}{2}\right)\right)^2 \bmod p.$$

Mas

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

logo,

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

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

.

Como $p \equiv 1 \ mod\ 4$, ou seja, $p = 4m + 1$, em que $m \in Z$, pode-se escrever

$$\frac{(p+1)}{2} = \frac{(4m+1+1)}{2} = \frac{(4m+2)}{2} = 2m + 1.$$

Assim,

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

Como

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

então,

$$.\left(1.\,2.....\left(\frac{(p-1)}{2}\right)\right)^2 + 1 \equiv 0 \ mod\ p.$$

Substituindo $.\left(1.\,2.....\left(\frac{(p-1)}{2}\right)\right)$ por a, tem-se que:

$$a^2 + 1 \equiv 0 \ mod\ p.$$

Seja a uma solução para a equação $a^2 + 1 \equiv 0 \mod p$. Então $p \nmid a$, pois se $p \mid a$, tem-se $a^2 \equiv 0 \mod p$. Somando 1 a ambos os termos da equação, obtém-se $a^2 + 1 \equiv 1 \mod p$ e daí $0 \equiv 1 \mod p$, o que é falso. Pelo teorema de Thue (***Teorema 3.4.1***): existe $x, y \in \{1, 2, \ldots, \lfloor\sqrt{P}\rfloor\}$ tal que $ax \equiv \pm y \mod p$.

Multiplicando ambos os termos da equação $a^2 + 1 \equiv 0 \mod p$ por x^2, obtém-se:

$$a^2x^2 + x^2 \equiv 0 \mod p.$$

Substituindo a^2x^2 por y^2, pois $a^2x^2 \equiv y^2 \mod p$, obtém-se:

$$a^2x^2 + x^2 = y^2 + x^2 \equiv 0 \mod p.$$

Assim, conclui-se que $x^2 + y^2 = m.p$ para um $m \in Z$. Lembrando que $x, y \leq \lfloor\sqrt{P}\rfloor$, então $x^2, y^2 \leq \lfloor\sqrt{P}\rfloor^2 < (\sqrt{p})^2 = p$, logo $x^2 + y^2 < 2p$. Como $p \mid x^2 + y^2$ então $m = 1$, e como consequência chega-se a conclusão de que p pode ser escrito como soma de dois quadrados, isto é, $x^2 + y^2 = p$.

Exemplos: p = 2 = $1^2 + 1^2$, p = 4.9 + 1 = 37 = $6^2 + 1^2$.

Lema 4.2. Se u e w são escritos cada um como soma de dois quadrados, então o produto $u.w$ também será.

Demonstração:

Escrevendo u e w como soma de dois quadrados, $u = a^2 + b^2$ e $w = c^2 + d^2$, em que a, b, c e d pertencem ao conjunto dos números inteiros. Deve-se mostrar que $u.w$ também pode ser representado por uma soma de dois quadrados, isto é, que existem r e s inteiros tais que $u.w = r^2 + s^2$. Efetuando o produto $u.w$, obtém-se:

$$u.w = (a^2 + b^2).(c^2 + d^2)$$

$$u.w = a^2.c^2 + a^2.d^2 + b^2.c^2 + b^2.d^2$$

$$u.w = a^2.c^2 + b^2.d^2 + a^2.d^2 + b^2.c^2$$

Somando ao 2º membro ***(2abcd)*** e ***(– 2abcd)***, obtém-se:

$$u.w = a^2.c^2 + 2abcd + b^2.d^2 + a^2.d^2 - 2abcd + b^2.c^2.$$

$$u.w = (ac + bd)^2 + (ad - bc)^2.$$

Portanto, sendo $r = ac + bd$ e $s = ad - bc$, chega-se a conclusão de que $u.w = r^2 + s^2$.

Exemplo: 493 = 17.29 em que $17 = 1^2 + 4^2$ e $29 = 2^2 + 5^2$, portanto $493 = (1.2 + 4.5)^2 + (1.5 - 4.2)^2 = 22^2 + 3^2$.

Teorema 4.2. Seja $n \in N$, escrito na forma $n = 2^c.p_1^{a_1}.p_2^{a_2}....p_r^{a_r}.q_1^{b_1}.q_2^{b_2}....q_s^{b_s}$ com $c \geq 0$, $a_1, \ldots, a_r, b_1, \ldots, b_s \in N$, $p_1, \ldots, p_r$ números primos distintos congruentes a 1 módulo 4 e $q_1, \ldots, q_s$ números primos distintos congruentes a 3 módulo 4, $r, s \geq 0$. Então n é soma de dois quadrados, se e somente se, todos os expoentes $b_1, b_2, \ldots, b_s$ são pares.

Demonstração:

i) Pelo ***Teorema 4.1***., já se provou que para $p = 2 = 1^2 + 1^2$ e p um número primo congruente a 1 modulo 4 é uma soma de dois quadrados, consequentemente, 2^c e $p^{a_1}, p^{a_2}, ..., p^{a_r}$ também podem ser escritos como soma de dois quadrados. Agora, basta provar que para todos os $q_1, \ldots, q_s$ números primos distintos congruentes a 3 módulo 4, $s > 0$, todos os expoentes $b_1, b_2, \ldots, b_s$ são pares. Se todo fator $q_s \equiv 3 \bmod 4$ se apresentar com expoente $b_s = 2\beta$, ou seja, par, tem-se $q^{2\beta} = (q^2)^\beta = (q^2 + 0^2)^\beta$, portanto q_s pode ser escrito como soma de dois quadrados e, consequentemente, pelo ***Lema 4.2***, quando $n = 2^c.p_1^{a_1}.p_2^{a_2}....p_r^{a_r}.q_1^{b_1}.q_2^{b_2}....q_s^{b_s}$, tem-se satisfeita a hipótese de que n pode ser escrito como soma de dois quadrados.

ii) Sendo $q \equiv 3 \bmod 4$ um número primo. Escrevendo $n = a^2 + b^2$ e supondo que q divida n com q^k a maior potência de q que divide tanto a como b, pode-se escrever a e b como sendo

$a = q^k.a_1$ e $b = q^k.b_1$. Como $n = a^2 + b^2$, obtém-se ao substituir a e b pelos seus respectivos valores,

$$n = (q^k.a_1)^2 + (q^k.b_1)^2$$

$$n = q^{2.k}.a_1^2 + q^{2.k}.b_1^2$$

$$n = q^{2.k}(a_1^2 + b_1^2)$$

$$\frac{n}{q^{2.k}} = a_1^2 + b_1^2$$

Como q não divide $\frac{n}{q^{2.k}}$, então q não divide a_1 e nem b_1. Assim, $q^{2.k}$ é a maior potência de q que divide n e ,portanto, $b_s = 2.k$.

Exemplo: $306 = 2.3^2.17 = (1^2 + 1^2).(3^2 + 0^2).(1^2 + 4^2) = [(1.3 + 1.0)^2 + (1.0 – 1.3)^2].(1^2 + 4^2) = (3^2 + 3^2).(1^2 + 4^2) = (3.1 + 3.4)^2 + (3.4 – 3.1)^2 = 15^2 + 9^2$.

5 CONCLUSÃO

Procurou-se neste trabalho determinar quais os números inteiros que podem ser ou não escritos como soma de dois quadrados.

Introduziram-se várias demonstrações procurando transmitir de maneira simples, porém sem perder a exigência formal das definições importantes, tais como: divisibilidade, números primos, congruência e demonstrações a fim de que qualquer aluno do ensino médio, que possua o mínimo de entendimento sobre matemática, consiga entender e ampliar seus conhecimentos.

Buscou-se ressaltar, através da simplicidade, a importância dos conceitos, das propriedades, das demonstrações dos encadeamentos lógicos, do seu aspecto dedutivo, fundamentando seu caráter instrumental, tornando válidas suas intuições e conjecturas para que se pudesse comentar no Ensino Médio. Tornando a curiosidade uma forma de motivação, para que o aluno procure despertar o raciocínio lógico em busca de condições para obter números inteiros não negativos os quais possam ser escritos como uma soma de dois quadrados e, além disso, procure determinar uma justificativa.

A apresentação das condições suficientes que um número inteiro, não negativo, requer para ser escrito como soma de dois quadrados, pode ser apresentada ao aluno do ensino médio em paralelo com algumas áreas da matemática, como aritmética, geometria, congruência, função e, até mesmo, números complexos, conforme se observa nos exemplos abaixo.

- Número que não pode ser escrito como soma de dois quadrados é o número 7, pois é escrito da forma $4m + 3$ e, ainda mais, que os números escritos desta maneira formam uma função polinomial do 1º grau e são representados por uma sequência crescente denominada progressão aritmética, cuja razão vale 4.
- Sabe-se que $2 = 1^2 + 1^2$ e que $17 = 4^2 + 1^2$ e que o seu produto deve ser expresso como soma de dois quadrados. Na verdade $34 = 5^2 + 3^2$. Existe uma maneira prática de descobrir como isso é possível. Faz-se necessário incentivar o aluno para que busque o porquê de tal situação e consiga chegar a uma fórmula matemática.
- Sabe-se que cada solução (x, y) da equação $x^2 + y^2 = N$ pode ser representada por um ponto no plano cartesiano no qual esse ponto possui coordenadas inteiras não negativas e que essa equação representa uma circunferência, cujo centro encontra-se na origem do plano cartesiano de raio N, exceto para o ponto (0,0). E que cada círculo possui uma área obtida pelo produto do π (pi) por N.

- Marcando todos os pares (x,y) solução da equação $x^2 + y^2 = N$, pode-se obter a solução de uma questão relacionada, buscando uma resposta surpreendente para a seguinte pergunta : Quantas maneiras pode um número inteiro não negativo ser escrito como soma de dois quadrados?

Tendo como pressupostos esses exemplos, fica evidente a possibilidade em relacionar os assuntos matemáticos citados nesta dissertação com os conteúdos de matemática estudados no Ensino Médio. Dessa forma, é possível aguçar o interesse pela descoberta, pela busca do aprendizado, tornando a matemática uma ciência investigativa, uma ciência prazerosa.

Assim, espera-se que esta dissertação venha a contribuir com os professores e alunos do Ensino Médio, para que possam usufruí-la como fonte de pesquisa.

REFERÊNCIAS

DANTE, Luiz Roberto. **Restos, congruência e divisibilidade.** RPM v.10, SBM, RJ, 1987.

DODLEY, Underwood, **Elementary Number Theory**. USA, 1969.

HARDY, G.H.; WRIGHT, E.M.. **An introduction to the theory of numbers.** New York : John Wiley, 1960.

HEFEZ, Abramo. **Elementos de aritmética.** Rio de Janeiro : SBM, 2006.

JUNIOR, G.O.L. **Números inteiros, Congruências e Somas de Quadrados.**2013. 58 f. Tese (mestrado) – Departamento de Matemática, Universidade Federal do Ceará, Fortaleza, 2013.

LIMA, Elon Lages. **Análise Real.** volume 1. Rio de Janeiro: Coleção matemática universitária. Outubro, 2008.

MUNIZ NETO, Antonio Caminha. **Tópicos de matemática elementar:** teoria dos números. Rio de Janeiro: SBM, 2012. v.5.

ROSEN, Kenneth H., **Elementary Number Theory and Its Applications**. USA, 1986.

SANTOS, J. P. de O. **Introdução a teoria dos números**. Rio de Janeiro : IMPA, 1998.

SERRE, J.A., Course D'algèbre Supérieure, Paris, 1879.