UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I – CAMPINA GRANDE
CENTRO DE CIÊNCIAS E TECNOLOGIA - CCT
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

ISAEDJA FERREIRA DE ANDRADE

ALGUNS RESULTADOS SOBRE NÚMEROS PRIMOS

CAMPINA GRANDE – PB
2013

ISAEDJA FERREIRA DE ANDRADE

ALGUNS RESULTADOS SOBRE NÚMEROS PRIMOS

Monografia apresentada ao Curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, como parte dos requisitos exigidos para obtenção do título de Licenciado em Matemática.

Orientador: Prof. Dr. Vandenberg Lopes Vieira

CAMPINA GRANDE – PB
2013

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL – UEPB

A553a Andrade, Isaedja Ferreira de.

Alguns resultados sobre números primos [manuscrito] / Isaedja Ferreira de Andrade. – 2013.

48 f.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) – Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2013.

"Orientação: Prof. Dr. Vandenberg Lopes Vieira, Departamento de Matemática".

1. Números inteiros. 2. Números primos. 3. Aritmética. I. Título.

21. ed. CDD 510

ISAEDJA FERREIRA DE ANDRADE

ALGUNS RESULTADOS SOBRE NÚMEROS PRIMOS

Monografia apresentada no Curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, em cumprimento às exigências para obtenção do Título de Licenciado em Matemática.

BANCA EXAMINADORA

Prof. Dr. **Vandenberg Lopes Vieira**
Departamento de Matemática – CCT/UEPB
Orientador

Prof. Dr. Juarez Dantas de Souza
Departamento de Matemática – CCT/UEPB (10)
Examinador

Maria Isabelle Silva

Prof. Dra. Maria Isabelle Silva
Departamento de Matemática – CCT/UEPB
Examinadora

Campina Grande, 17 de outubro de 2013

A toda minha família e em especial
aos meus pais por todo o incentivo.
DEDICO

Agradecimentos

A Deus, fonte de vida, por iluminar meu caminho e sempre me dar forças para seguir sempre em frente.

A meus pais por todas as noites que me esperaram, pela confiança em mim e por terem feito de suas vidas uma completa doação para que eu atingisse meus objetivos.

Aos meus irmãos por toda a ajuda durante o curso e em tantos momentos em minha vida.

Ao meu orientador, Vandenberg Lopes, por sua constante paciência, disponibilidade, entusiasmo, pelas discussões enriquecedoras e pela dedicação que possibilitaram a conclusão do presente trabalho. Obrigado também pelo apoio durante todo o curso.

A todos os meus ex-professores, pela contribuição com seus conhecimentos para minha formação acadêmica, profissional e pessoal.

A Eder Cabral, pelas palavras de incentivo e pela confiança em mim.

Aos meus grandes amigos que sempre me incentivaram e me proporcionaram momentos de distração, imprescindíveis ao bom andamento deste estudo. E aos amigos de curso, por todo apoio durante toda essa jornada.

Enfim, a todos que de alguma maneira contribuíram para a execução desse trabalho.

Resumo

Neste trabalho, abordamos alguns resultados sobre os números primos, que formam uma classe de números inteiros bastante especial. As diversas aplicações e as conjecturas sobre os primos, ainda sem demonstração, foram a motivação principal de escolha do tema. Por se tratar de um trabalho de conclusão de curso, o texto foi planejado para servir de suporte a alunos de graduação, motivando-os também na pesquisa sobre o conteúdo. Por isso, consideramos principalmente os resultados básicos, os quais, em geral, são vistos em um curso de introdução em Teoria dos Números. Dentre eles, destacam-se o Teorema Fundamental da Aritmética (a essência da aritmética) e o Teste de Primalidade.

Palavras-chave: Números Inteiros, Números Primos, Conjecturas sobre Primos.

Sumário

Introdução

A Teoria dos Números é um dos ramos mais importantes e belos da matemática. Ela tem como objetivo central o estudo dos números inteiros, bem como suas propriedades. Referências indicam que a mais ou menos 500a.C. os gregos antigos já estudavam esses números. Além deles, diversos estudiosos de todo o mundo contribuiram para o desenvolvimento dessa área. Muitas vidas dedicadas, muitas conquistas, muitas frustrações e ainda, muitos mistérios cercavam e cercam esses números. E o que antes parecia desafiar e fascinar apenas matemáticos, depois de 2500 anos passa a ter importancia para estudiosos de diversas áreas.

Este trabalho trata de uma das classes de números que por muitos é considerada a mais importante: Os números primos, ou primários.

O estudos desses números sempre despertou a curiosidade e o fascinio dos matemáticos. Atribui-se, de acordo com documentos antigos, a Pitágoras de Samos (VI a.C.), matemático grego, os primeiros estudos sobre os números primos. Apesar de que em um papiro egício conhecido como Papiro de Rhind, de cerca de 1650 a.C. os números primos eram escritos de maneira diferentes dos demais, o que poderia ser um indício de que os antigos egípcios já haviam observado esses números de certa forma. Apesar de citado, Pitágoras é uma das figuras mais misteriosas da matemática e não existem registros de seus trabalhos, apenas em documentos posteriores a sua existencia citam-o. Contudo, o mais antigo registro que citam os números primos e que chegou aos nossos dias é uma coleção denominada "Os Elementos"do grego Euclides de Alexandria (350d.C.), um dos primeiros grandes matemáticos que se sabe. Essa coleção era composta por 13 volumes. Euclides dedicou os livros VII e IX a conceitos sobre Teoria dos Números. Considerado a coleção didática mais bem sucedida de toda a história, de acordo com Encyclopedia of Ancient Greece (2006) por Nigel Guy Wilson, página 278. Além disso, essa obra matemática é conhecida também por ser o segundo maior best seller mundial, sendo o primeiro a Bíblia. No livro, Euclides define o que são números primos, apresentou algumas propriedades e provou através de uma ingênua demonstração que esses números são infinitos.

Um matemático que contribuiu para o avanço do estudo dos números primos foi Carl Friedrich Gauss. Por volta do século XXVIII, Gauss ganhara um livro de tabelas

matemáticas de presente de aniversário de 15 anos. Entre as tabelas existia uma que lhe chamou a atenção, a tabelas de números primos. Eles passou horas analisando e as tabelas pareciam começar a revelar seus segredos para o brilhante jovem. Ele começou a contar a quantidade de primos existentes em blocos de 1000 e construiu uma estrutura que revolucionou o estudos dos primos. Gauss percebeu que cada vez que aumentavam os números inteiros, diminuia a probabilidade de ser encontrar números primos (visto que eles surgiam ao acaso, ele estudava, ao invés de fórmulas matemáticas de se obter primos, a probabilidade de ser encontrar um número primo nesses blocos numéricos) e mais, ele descobriu a proporção com que eles diminuem. Ele acreditava que existia certa regularidade na forma com que os primos decresciam. Mas ele não sabia como explicar esse fato. Essas e outras descobertas de Gauss eram mantidas em seu diário secreto, ele apenas publicava o que havia certeza de fato. Por suas contribuições e pela amplitude que elas alcançam, Gauss é considerado o Príncipe da Matemática.

Outro matemático que contribuiu para aumentar ainda mais o fascínio dos matemáticos pelos números primos foi o alemão Bernhard Riemann. Em 1859, Riemann conseguiu mostrar o que Gauss havia iniciado anteriormente a quantidade de números de primos entre 1 e n, quando n é muito grande, é aproximadamente $\frac{n}{\ln x}$. Riemann trabalhava em uma função conhecida como função Zeta quando percebeu uma relação existente com os números primos. Ele observou que os zeros dessa função tinham uma conexão com a forma com que os primos são distribuidos mas não sabia como demonstrar isso. Sua descoberta se equipara a primeira fórmula de Einstein, ela dava harmonia a distribuição dos números primos. Alguns matemáticos como por exemplo, G. H. Hardy (1877-1947) e Srinivasa Ramanujan (1887 - 1920) mostraram que essa hipótese de Riemann era verdadeira para uma infinidade de números primos mas isso ainda não é o bastante, a hipótese necessita de uma demonstração geral.

O matemático Alan Turing, conhecido como o Pai da Ciência da Computação, trabalhou também na hipótese de Riemann. Ele construiu uma máquina que explorava o gráfico da função zeta em busca de zeros da função que pudessem tornar a hipótese falsa. Mas, durante a Segunda Guerra Mundial, Turing e outros matemáticos passaram a trabalhar para inteligência britânica Bletchley Park. Ele era responsável pela criptoanálise, arte de tentar descobrir o texto cifrado e/ou a lógica utilizada em sua encriptação da frota naval alemã. O seu trabalho com números primos contribuiu para decifrar códigos dos inimigos. Após a Segunda Guerra, construiu o prótotipo do computador moderno, uma máquina que auxiliaria em diversos cálculos matemáticos. Com essa máquina, Turing iniciou uma nova era para os números primos, onde os computadores ultrapassavam os homens nesse estudo. Foi em 1952 que um computador descobriu os primeiros números primos.

Os computadores atuais contribuem para o estudo dos números primos, bem como a exploração da Hipótese de Hiemann, mas apesar de aumentarem a evidência de que essa última é verdadeira, ainda não se tem uma demonstração geral.

Outras questões que envolvem números primos ainda continuam surgindo. Em 1972, um americano Hugh Montgomery percebeu uma relação entre a energia de um núcleo de um atómo de urano com a Hipótese de Riemann e assim, com os números primos, unindo dessa forma os físicos ao mistério desses números. Agora, os blocos básicos da matemática e os da física parecem corresponder-se em termos de comportamento, o que introduz uma nova hipótese, ou um novo olhar para a mesma hipótese anterior.

Os números primos também desempenham um papel importante na comunicação eletrônica. Em uma transação online por exemplo, utilizamos números primos para codificar as informações de nosso cartão de crédito. Esse sistema tem como base a dificuldade de se verificar os primos constituintes de uma sequencia numérica. Uma solução que diminuisse essa dificuldade ou acabasse com ela traria problemas para toda a matemática e para diversas áreas como a segurança de sistemas.

Em 1998 foi fundado o Clay Mathematics Institute, com o objetivo de desenvolver e divulgar conhecimentos matemáticos e apoio dos melhores centros de pesquisa, como a Universidade Harvard e o Instituto de Tecnologia de Massachusetts. O Instituto Clay oferece, e não é a toa, um prêmio de 1 milhão de dólares para aquele que desvendar o mistério dos números primos.

A motivação de se trabalhar esse tema vem da importância que os números primos exercem até hoje sobre a matemática, e agora, sobre outras áreas do conhecimento,por se tratar de um conteúdo que ainda deixa questões não resolvidas, pelo fascinio pelos mesmos e mais, com o objetivo de servir como motivação para alunos de graduação ao estudo dos mesmos.

No Capítulo 1 será apresentado os conjunto dos números inteiros, bem como suas propriedades necessárias ao entendimento do capítulo posterior. No Capítulo 2 será mostrado algumas curiosidades e propriedades referentes aos números primos, bem como algumas hipóteses ainda em aberto sobre os mesmos.

Capítulo 1

Os Números Inteiros

Vamos considerar inicialmente o conjunto numérico $\mathbb{N}$ formado pelos elementos que denominamos números naturais,

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

Os números naturais são, de fato, os mais familiares entre todos os conjuntos numéricos clássicos, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$[1]visto que sempre estiveram ligados às necessidades do homem de registrar e interpretar fenômenos que o cercavam.

Utilizaremos as propriedades e axiomas referentes a $\mathbb{N}$ em um ambiente mais amplo, destacando o conjunto dos números inteiros $\mathbb{Z}$, definido abaixo.

Indicaremos por $\mathbb{Z}$ o conjunto formado pelos números inteiros:

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

Fica evidente que $\mathbb{N}$ é um subconjunto de $\mathbb{Z}$, isto é, $\mathbb{N} \subset \mathbb{Z}$. Mas esse fato não é coincidência. Os números inteiros, assim como todos os outros conjuntos numéricos, surgiram a partir das necessidades operatórias do momento. Por exemplo, algumas operações de subtração em $\mathbb{N}$, não resultavam em elementos de $\mathbb{N}$: $4 - 9 = -5 \notin \mathbb{N}$. Isto motivou o surgimento do conjunto dos números inteiros. Podemos dizer então que $\mathbb{Z}$ é uma "ampliação de $\mathbb{N}$".

Além de $\mathbb{N}$, podemos destacar alguns subconjuntos de $\mathbb{Z}$:

$\mathbb{Z}^*$	$=$	$\{\ldots -3, -2, -1, 1, 2, 3 \ldots\}$	(elementos não nulos de $\mathbb{Z}$).
$\mathbb{Z}_+$	$=$	$\{0, 1, 2 \ldots\}$	(elementos não negativos de $\mathbb{Z}$).
$\mathbb{Z}_+^*$	$=$	$\{1, 2 \ldots\}$	(elementos positivos de $\mathbb{Z}$).
$\mathbb{Z}_-$	$=$	$\{\ldots -3, -2, -1, 0\}$	(elementos não positivos de $\mathbb{Z}$).
$\mathbb{Z}_-^*$	$=$	$\{\ldots -3, -2, -1\}$	(elementos negativos de $\mathbb{Z}$).

O conjunto $\mathbb{Z}$ munido das operações fundamentais de adição e multiplicação denotadas por $+$ e $\cdot$, respectivamente possuem algumas propriedades elementares que passamos a descrever a seguir.

(A adição e multiplicação são comutativas) Para quaisquer $a, b \in \mathbb{Z}$, temos

$$a + b = b + a \quad \text{e} \quad a \cdot b = b \cdot a.$$

(A adição e multiplicação são associativas) Dados $a, b \in \mathbb{Z}$, valem

$$a + (b + c) = (a + b) + c \quad \text{e} \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(A adição possui elemento neutro) Existe único elemento em $\mathbb{Z}$, que indicaremos por 0, e chamado zero, tal que

$$a + 0 = a, \quad \forall\ a \in \mathbb{Z}.$$

(A multiplicação possui elemento neutro) Existe único elemento em $\mathbb{Z}$, que indicaremos por 1, chamado um, tal que

$$a \cdot 1 = a, \quad \forall\ a \in \mathbb{Z}$$

Além desses axiomas semelhantes à ambas operações temos:

(Existência de inverso aditivo) Dado um inteiro a, existe um único elemento $-a \in \mathbb{Z}$, chamado inverso aditivo de a tal que:

$$a + (-a) = 0, \quad \forall a \in \mathbb{Z}.$$

(Lei do cancelamento do produto) Para quaisquer $a, b, c \in \mathbb{Z}$ com $b \neq 0$, temos

$$a \cdot b = b \cdot c \Rightarrow a = c.$$

(Lei do cancelamento da adição) Para quaisquer $a, b, c \in \mathbb{Z}$,

$$a + b = a + c \Rightarrow b = c.$$

(Distributividade da multiplicação sobre a adição) Para quaisquer $a, b, c \in \mathbb{Z}$ com $b \neq 0$, temos

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Observao 1.1 *Notemos que diferente do que ocorre sobre os conjuntos $\mathbb{Q}$, $\mathbb{R}$, e $\mathbb{C}$ uma equação linear em $\mathbb{Z}$,*

$$ax = b$$

com a, $b \in Z$ e $a \neq 0$, nem sempre possui solução inteira. Isso só ocorre quando b for um múltiplo de a. Por exemplo, $2x = 7$ não tem solução em $\mathbb{Z}$, já $3x = 12$ possui $x_0 = 4$ como solução.

A partir desses axiomas mostraremos algumas propriedades com respeito às operações de multiplicação e adição.

Proposio 1.1 *Dados $a, b \in \mathbb{Z}$, temos:*

(1) $a \cdot 0 = 0$.

(2) *Se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.*

Demonstração: (1) Como $0 = 0 + 0$ então

$$a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = a \cdot 0 + 0.$$

Assim,

$$a \cdot 0 + a \cdot 0 = a \cdot 0 + 0.$$

Portanto, $a \cdot 0 = 0$.
(1) Pel item (1), podemos escrever $0 = a \cdot 0$. Como por hipótese $a \cdot b = 0$, então $a \cdot b = a \cdot 0$. Se $a = 0$ a proposição está demonstrada. Caso contrário, pela lei do cancelamento do produto temos que $b = 0$. Dessa forma, ou $a = 0$ ou $b = 0$. ■

Além das operações de adição e multiplicação definidas sobre $\mathbb{Z}$, existe também uma relação definida em termos da adição de modo que, sendo a e b números inteiros, dizemos que a é menor do que b, em símbolos $a < b$, quando existe $m \in \mathbb{N}$ tal que

$$b = a + m.$$

Com o mesmo significado, dizermos que b é maior do que a e escrevemos $b > a$. No caso em que a é menor ou igual a b usamos a notação $a \leqslant b$.

Dizemos que essa relação é uma "relação de ordem". Denotandomos essa relação com o símbolo $\leqslant$. Passaremos a enunciar agora os axiomas referentes a essa relação.

(A relação "$\leq$"é reflexiva) Dado $a \in \mathbb{Z}$, temos que $a \leqslant a$.

(A relação "$\leq$"é anti simétrica) Dados $a, b \in \mathbb{Z}$, se $a \leqslant b$ e $b \leqslant a$ então $a = b$.

(A relação "$\leq$"é transitiva) Dados $a, b, c \in \mathbb{Z}$, se $a \leq b$ e $b \leq c$ então $a \leq c$.

(Tricotomia) Quaisquer que sejam $a, b, c \in \mathbb{Z}$ podem ocorrer $a < b$ ou $a = b$ ou $a > b$.

(Monotonicidade da adição) Quaisquer que sejam a, b e $c \in \mathbb{Z}$, se $a \leq b$ então $a + c \leq b + c$

(Monotonicidade da multiplicação) Quaisquer que sejam $a, b, c \in \mathbb{Z}$ com $a \leq b$ e $0 \leq c$ tem-se que $ac \leq bc$.

Proposio 1.2 *Para todo $a \in \mathbb{Z}$ temos:*

(1) *Se $a \leq 0$ então $-a \geq 0$, $\forall\ a \in \mathbb{Z}$.*

(2) $a^2 \geq 0$, $\forall\ a \in \mathbb{Z}$.

(3) $1 > 0$.

Demonstração: (1) Se $a \leq 0$ então, temos $a + (-a) \leq 0 + (-a)$, assim $0 \leq (-a)$ ou seja, $-a \geq 0$.
(2) Faremos inicialmente a demonstração para o caso em que $a \geq 0$. Multiplicando os membros da desigualdade por a temos que $a \cdot a \geq 0 \cdot a$ ou seja, $a^2 \geq 0$. Agora, para o caso em que $a < 0$ temos que $-a > 0$. Assim, multiplicando ambos os membros da desigualdade por $-a$, segue que

$$(-a) \cdot (-a) > 0 \cdot (-a)$$

ou seja, $(-a)^2 = a^2 > 0$.
(3) Como $1 = 1^2$ segue que $1^2 > 0$ então $1 > 0$. ■

Definio 1.1 *Chamaremos de **valor absoluto** de um número inteiro a, denotado por $|a|$, da seguinte forma*

$$\begin{cases} |a| = a \quad se \quad a \geq 0 \\ |a| = -a \quad se \quad a < 0. \end{cases}$$

Nota-se que, por definição, $|a| \geq 0$, $\forall\ a \in \mathbb{Z}$. Além disso, a igualdade ocorre se, e somente se, $a = 0$. Dessa forma, o valor absoluto de 5 ou $|5| = 5$, uma vez que $5 > 0$; já $|-2| = -(-2) = 2$, pois $-2 < 0$.

Podemos ainda escrever o valor absoluto de um número inteiro a como sendo a raíz quadrada de a^2, ou seja, $|a| = \sqrt{a^2}$.

Proposio 1.3 *Para $a, b, c \in \mathbb{Z}$, valem as propriedades:*

(1) $|a \cdot b| = |a| \cdot |b|$.

(2) $-|a| \leq a \leq |a|$.

(3) $|a| \leq c \Leftrightarrow -c \leq a \leq c$.

(4) $|a + b| \leq |a| + |b|$. **(Desigualdade Triangular)**

Demonstração: (1) Se $a \geq 0$ e $b \geq 0$, então $ab \geq 0$. Assim,

$$|a \cdot b| = ab = |a| \cdot |b| .$$

Se $a \geq 0$ e $b \leq 0$, então $ab \leq 0$. Logo,

$$|a \cdot b| = -(ab) = a(-b) = |a| \cdot |b| .$$

Os casos $a \leq 0$, $b \geq 0$ e $a \leq 0$, $b \leq 0$ são tratados de modo similar.
(2) O resultado desse item é obtido diretamente da definição.
(3) Suponhamos que $|a| \leq c$. Temos que $-|a| \geq -c$. Assim, do item (2), obtemos

$$-c \leq -|a| \leq a \leq |a| \leq c,$$

ou seja,

$$-c \leq a \leq c.$$

Reciprocamente, vamos supor que $-c \leq a \leq c$. Se $a \geq 0$, então

$$|a| = a \leq c.$$

Se $a < 0$, então

$$|a| = -a \leq c.$$

(4) Pelo item (2), temos que

$$-|a| \leq a \leq |a| \quad \text{e} \quad -|b| \leq b \leq |b| .$$

Somando membro a membro estas desigualdades, segue que

$$-(|a| + |b|) \leq a + b \leq |a| + |b| .$$

Portanto, pelo item (3),

$$|a + b| \leq |a| + |b| .$$

■

1.1 Princípio da Boa Ordenação

A partir de agora, a hipótese básica inicial sobre os inteiros que destaremos é o Princípio da Boa Ordenação. Trata-se de uma forte ferramenta usada em algumas demonstrações matemáticas. Esse princípio será utilizado como fundamento para uma série de resultados sobre os números inteiros.

Definio 1.2 *Seja X um subconjunto não-vazio de $\mathbb{Z}$. Diz-se que X é* ***limitado inferiormente*** *quando existir um elemento $x_0 \in \mathbb{Z}$ tal que*

$$x_0 \leq x, \quad \forall\, x \in X.$$

Diz-se também que X é limitado inferiormente por x_0 e que este é um ***limitante inferior*** *de X.*

Exemplo 1.1 *O conjunto $X_1 = \{1, 2, 3, 4\}$ é limitado inferiormente, pois $x_0 = 1$ é um limitante inferior de X_1. Em geral, todo subconjunto finito não-vazio X de Z é limitado inferiormente. Já o conjunto $X_2 = \{\ldots, -2, -1, 0, 1, 2, \}$ não tem um limitante inferior.* ♣

Nota-se que um limitante inferior de um conjunto X não necessariamente pertence a X.

Axioma 1.1 (Princípio da Boa Ordenação – PBO) *Todo subconjunto não-vazio X de $\mathbb{Z}$ limitado inferiormente possui um menor elemento (ou elemento mínimo).*

Para o conjunto dos naturais, o PBO se reduz à afirmação: *todo subconjunto não-vazio X de $\mathbb{N}$ possui um menor elemento.*

Diferente de um limitante inferior, um elemento mínimo de um conjunto X, por definição, pertence a X.

Proposio 1.4 *Na condição do axioma anterior, o elemento mínimo $x_0 \in X$ é único.*

Demonstração: Se x_0 e y_0 são elementos mínimos de X, então $x_0 \leq y_0$ e $y_0 \leq x_0$. Mas, isto em $\mathbb{Z}$ implica em $x_0 = y_0$, poia a relação " $\leq$ " é anti-simétrica. ■

Indicaremos o elemento mínimo x_0 de X por

$$x_0 = \min X.$$

Corolrio 1.1 *Seja a um número inteiro. Se $a > 0$, então $a \geq 1$.*

Demonstração: Provaremos a afirmação por absurdo. Assim, suponhamos que exista $m \in \mathbb{Z}$ com $0 < m < 1$. Desse modo, o conjunto $X = \{m \in \mathbb{Z} : 0 < m < 1\} \subset \mathbb{Z}$ é não-vazio e limitado inferiormente e, pelo PBO, X possui um menor elemento x_0. Como $x_0 \in X$, segue que $0 < x_0 < 1$; multiplicando estas desigualdades por x_0, obtemos

$$0 < x_0 < 1 \Rightarrow 0 < x_0^2 < x_0 < 1,$$

ou seja, $0 < x_0^2 < 1$, o que implica que $x_0^2 \in X$ e $x_0^2 < x_0$, contrariando a minimalidade de x_0. ■

Corolrio 1.2 *Seja a e b inteiros quaisquer. Se $a > b$, então $a \geq b + 1$.*

Demonstração: Como $a - b > 0$, então pela proposição anterior, $a - b \geq 1$, ou seja, $a \geq b + 1$. ■

1.2 Indução Matemática

No sentido denotativo do termo, indução é um raciocínio em que de casos particulares se tira uma conclusão genérica. O que nos permite concluir se uma afirmação é verdadeira ou falsa.

Partiremos do Princípio da Boa Ordenação e consideraremos agora o Princípio da Indução Finita ou Princípio de Indução Matemática. Esse resultado é utilizado quando desejamos demonstrar que certa propriedade é válida sobre um conjunto de $\mathbb{Z}$ limitado inferiormente.

Se queremos, por exemplo, provar que uma declaração é verdadeira para todos os números naturais, provar que é verdadeira para um grande número de casos particulares não nos permite concluir que ela é válida para todos. Pelo Princípio de Indução Matemática, primeiramente devemos mostrar que a declaração é verdadeira para o primeiro número. Depois devemos mostrar que se vale para o primeiro número então valerá também para o subsequente. Se for verdadeira para o segundo então será para o seu sucessor e assim por diante. De forma geral, deve-se mostrar que se a declaração vale para o n-ésimo número, então valerá para o número seguinte $(n+1)$.

Chamaremos essa declaração de $P(n)$ de modo que $P(n)$ é uma sentença aberta que depende da variável n, elemento de um subconjunto de $\mathbb{Z}$, limitado inferiormente.

Teorema 1.1 (Indução Finita – 1ª Forma) *Seja $P(n)$ uma sentença sobre o conjunto $\{n \in \mathbb{Z} : n \geq n_0\}$, em que $n_0 \in \mathbb{Z}$, tal que:*

(1) *$P(n_0)$ é verdadeira.*

(2) *Se $P(n)$ é verdadeira para $n \geq n_0$, então $P(n+1)$ também é verdadeira.*

Logo, $P(n)$ é verdadeira para todo $n \geq n_0$.

Demonstração: Vamos considerar o seguinte conjunto

$$X = \{n \in \mathbb{Z} : n \geq n_0 \text{ e } P(n) \text{ é falsa}\}.$$

Suponhamos por absurdo que $X \neq \emptyset$. Como X é limitado inferiormente (por n_0, por exemplo), então pelo PBO, existe $m_0 \in X$ (elemento mínimo) tal que

$$m_0 \leq n, \quad \forall\, n \in X.$$

Como $m_0 \in X$, temos que $m_0 \geq n_0$ e $P(m_0)$ é falsa. Logo, $m_0 \neq n_0$, pois, por hipótese, $P(n_0)$ é verdadeira. Por conseguinte, $m_0 > n_0$ então, $m_0 - 1 \geq n_0$. Sendo m_0 o menor

elemento de X, segue que $m_0 - 1 \notin X$. Portanto, $P(m_0 - 1)$ é verdadeira; mas pela condição (2),

$$P(m_0 - 1 + 1) = P(m_0)$$

é verdadeira e, assim, $m_0 \notin X$, o que é uma contradição. Logo, $X = \emptyset$ e, portanto, $P(n)$ é verdadeira para todo $n \geq n_0$. ■

Exemplo 1.2 *Mostrar, usando indução finita, que*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}, \ \forall n \in \mathbb{N}.$$

Solução: Seja $P(n)$ a seguinte sentença sobre $\mathbb{N}$,

$$P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Como $1 = \frac{1(1+1)}{2}$, temos que $P(n_0 = 1)$ é verdadeira. Assim, por hipótese de indução, vamos supor que $P(n)$ seja verdadeira, e provemos que $P(n+1)$ também o é, ou seja,

$$P(n) \Rightarrow P(n+1).$$

Para $n + 1$, usando a hipótese de que $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$,

$$\begin{aligned} 1 + 2 + \cdots + n + 1 &= (1 + 2 + \cdots + n) + n + 1 \\ &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}, \end{aligned}$$

o que prova que $P(n+1)$ é verdadeira. Portanto, $P(n)$ é verdadeira para todo $n \geq 1$. ♣

Exemplo 1.3 *Provar que* $2^n \leq n!$ *para todo* $n \geq 4$, *em que* $n! = 1 \cdot 2 \cdots n$.

Solução: Consideremos

$$P(n) : 2^n \leq n!, \quad \forall n \geq 4.$$

É claro que $2^4 = 16 \leq 4!$, isto é, $P(n_0 = 4)$ é verdadeira. Suponhamos que $2^n \leq n!$, com $n \geq 4$. Assim,

$$2^{n+1} \leq 2^n \cdot 2 \leq n! \cdot 2.$$

Sendo $n \geq 4$, segue que $2 \leq n + 1$. Portanto, $n! \cdot 2 \leq n! \cdot (n+1) = (n+1)!$ e, por transitividade,

$$2^{n+1} \leq (n+1)!.$$

Desse modo, $P(n+1)$ é verdadeira e, por conseguinte, $P(n)$ é verdadeira para todo $n \geq 4$. ♣

De modo análogo, prova-se a segunda forma de indução finita.

Teorema 1.2 (Indução Finita – $2^{\underline{a}}$ Forma) *Seja $P(n)$ uma sentença sobre o conjunto $\{n \in \mathbb{Z} : n \geq n_0\}$, em que $n_0 \in \mathbb{Z}$, tal que:*

(1) *$P(n_0)$ é verdadeira.*

(2) *Se $P(m)$ é verdadeira para todo inteiro m tal que $n_0 \leq m \leq k$, então $P(k+1)$ é também verdadeira.*

Logo $P(n)$ é verdadeira para todo $n \geq n_0$.

1.3 Divisibilidade em $\mathbb{Z}$

Destacaremos algumas propriedades importantes relacionadas ao conceito de divisibilidade, sendo seu resultado principal o algoritmo da divisão, que é o meio mais eficiente de se calcular o máximo divisor comum entre inteiros.

Para evitar repetições de certas frases, as letras a, b, etc. indicarão nesta seção sempre números inteiros.

Diz-se que b **divide** a, que b é um **divisor** de a ou que a é um **múltiplo** de b, em símbolo, $b \mid a$, quando existir um inteiro c tal que

$$a = bc.$$

Para indicar que b não divide a, usa-se o símbolo $b \nmid a$. Assim,

$$b \mid a \Leftrightarrow a = bc \quad \text{para algum} \quad c \in \mathbb{Z}.$$

Por exemplo, $3 \mid 9$, $-7 \mid 21$ e $5 \nmid 22$. Além disso, $1 \mid a$ e $a \mid a$ para todo $a \in \mathbb{Z}$.

Chama-se um número $a \in \mathbb{Z}$ **par** quando $2 \mid a$; caso contrário, a é dito **ímpar**. Por exemplo, os números -4 e 14 são pares; enquanto 9 e 25 são ímpares. Diz-se que a e b têm a **mesma paridade** quando a e b são ambos pares ou são ambos ímpares.

Observao 1.2 *É fácil justificar o fato de, no estudo de divisibilidade, estarmos considerando o conjunto dos números inteiros, pois se estivessemos no conjunto dos números racionais ou reais todo número b poderia ser escrito da forma $b = a \cdot c$, com $a \neq 0$. Isso não despertaria nenhum interesse. Por exemplo, sabemos que em $\mathbb{Z}$, $2 \nmid 5$, mas se estivessemos falando em divisibilidade nos números reais, poderíamos escrever $5 = 2 \cdot c$, com $c = 5/2$.*

Observao 1.3 *O motivo de considerarmos $a \neq 0$ se deve ao fato que para este caso o valor de c é único. De fato, se $c' \in \mathbb{Z}$ é tal que $b = a \cdot c'$ então $a \cdot c' = a \cdot c$, o que implica $c = c'$. Portanto c, que chamaremos de quociente de b por a, é único e indicado por:*

$$c = b/a$$

Se admitissemos que $a = 0$,

$$0 \mid b \iff b = 0$$

(pois $b = 0 \cdot c$). Assim, o quociente não é único pois $0 \cdot c = 0$ para todo inteiro c. Por isso, consideraremos a partir de agora, que todos os divisores serão não-nulos, mesmo que não seja dito explicitadamente nos enunciados.

Lema 1.1 *Se $b \mid a$ e $a \neq 0$, então $|b| \leq |a|$.*

Demonstração: Se $b \mid a$, então existe $c \in \mathbb{Z}$ tal que $a = bc$. Logo, $|a| = |bc| = |b|\,|c|$. Como $c \neq 0$, então $|c| \geq 1$. Assim, multiplicando esta desigualdade por $|b|$, obtemos

$$|b| \leq |b|\,|c| = |a|\,.$$

■

Proposio 1.5 *Em $\mathbb{Z}$ valem as seguintes propriedades:*

(1) *Os únicos divisores de 1 são 1 e -1.*

(2) *Se $a \mid b$ e $b \mid a$, então $a = \pm b$.*

Demonstração: (1) Se b é um divisor de 1, então pelo Lema 1.1, temos que $|b| \leq 1$. Assim, $0 < |b| \leq 1$. Como não existe inteiro entre 0 e 1, concluímos que $|b| = 1$, isto é, $b = \pm 1$. A propriedade (2) segue imediatamente do item (1). ■

No próximo teorema, encontram-se outras propriedades elementares da divisibilidade.

Teorema 1.3 *A divisibilidade tem as propriedades:*

(1) $a \mid 0 \quad e \quad a \mid a$.

(2) *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

(3) *Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.*

(4) *Se $a \mid b$ e $a \mid c$, então $a \mid (mb + nc)$, $\forall\ m, n \in \mathbb{Z}$.*

Demonstração: Será demonstrado os itens (2) e (4).
(2) Por hipótese, temos $b = a\lambda_1$ e $c = b\lambda_2$ com $\lambda_1, \lambda_2 \in \mathbb{Z}$; substituindo o valor de b em $c = b\lambda_2$, temos $c = a\lambda_1\lambda_2$, ou seja, $a \mid c$.

(4) Para este item, temos por hipótese que $b = ak_1$ e $c = ak_2$ para inteiros k_1 e k_2. Portanto, quaisquer que sejam os inteiros m e n, $mb = amk_1$ e $nc = ank_2$, de modo que

$$mb + nc = a(mk_1 + nk_2) \Rightarrow a \mid (mb + nc).$$

■

O algoritmo da divisão (ou divisão Euclidiana), é considerado um dos mais familiares resultados dos inteiros, cujo resultado é base para muitas propriedades algébricas relevantes em $\mathbb{Z}$, será demonstrado tendo ponto de partida o seguinte lema:

Lema 1.2 (Propriedade Arquimediana) *Consideremos dois inteiros a e b com $b \neq 0$. Então, existe $n \in \mathbb{Z}$ tal que $nb \geq a$.*

Teorema 1.4 (Algoritmo da Divisão) *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então, existe únicos $q, r \in \mathbb{Z}$, tais que*

$$a = qb + r \quad com \quad 0 \leq r < |b|\,. \tag{1.1}$$

Demonstração: Consideremos o conjunto

$$S = \{a - bk : k \in \mathbb{Z}\}.$$

Pelo Lema 1.2, existe um inteiro n_0 tal que

$$-a \leq n_0(-b) \Rightarrow a \geq n_0 b \Rightarrow a - n_0 b \geq 0.$$

Desse modo, o conjunto L dado por

$$L = \{a - bq : q \in \mathbb{Z} \quad \text{e} \quad a - bq \geq 0\}$$

é não-vazio, pois $x = a - n_0 b \in L$. Como L é limitado inferiormente, segue pelo PBO que L possui menor elemento, digamos r. Como $r \in L$, então $r \geq 0$ e

$$r = a - bq \quad \text{com} \quad q \in \mathbb{Z}.$$

Mostremos agora que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Se $b > 0$, então $|b| = b$; logo, $r - b \geq 0$ e

$$r - b = a - qb - b = a - b(q + 1).$$

Daí, $r - b \in L$ e $r - b < r$, o que contradiz a minimalidade de r. Se $b < 0$, então $|b| = -b$; assim, $r + b \geq 0$ e

$$r + b = a - b(q - 1),$$

ou seja, $r + b \in L$ e $r + b < r$, o que é uma contradição. Desse modo, $a = qb + r$ com $q \in \mathbb{Z}$ e $0 \leq r < |b|$, o que prova a existência dos inteiros q e r. Para mostrarmos a unicidade desses inteiros, consideremos $q_1, r_1 \in \mathbb{Z}$ tais que

$$a = qb + r \quad \text{e} \quad a = q_1 b + r_1$$

com

$$0 \leq r < |b| \quad \text{e} \quad 0 \leq r_1 < |b|\,.$$

Assim,

$$qb + r = q_1 b + r_1 \Rightarrow r - r_1 = b(q_1 - q),$$

ou seja, $b \mid (r - r_1)$. Como $|r - r_1| < |b|$, segue que $r - r_1 = 0$, ou seja, $r = r_1$. Por conseguinte, $q_1 = q$, uma vez que $b \neq 0$. ■

Os inteiros q e r em (1.1) chamam-se **quociente** e **resto** da divisão Euclidiana de a por b, respectivamente. Às vezes, r também é dito **resto de** a **módulo** b.

Observao 1.4 *No Teorema* 1.4*, temos os seguintes casos particulares*:

(a) *Se* $a = 0$*, então* $q = r = 0$.

(b) *Se* $a > 0$ *e* $a < b$*, então* $q = 0$ *e* $r = a$.

Exemplo 1.4 *Determinar o quociente e resto da divisão de a por b quando:*

a) $a = 41 \quad e \quad b = 7$.

b) $a = -10 \quad e \quad b = 6$.

c) $a = -1243 \quad e \quad b = -4$.

Solução: a) Como $41 = 7 \cdot 5 + 6$ e $6 < 7$, então $q = 5$ e $r = 6$.
b) Para o caso em que $a = -10 < 0$ e $b = 6$, vamos efetuar a divisão natural de 10 por 6. Após isso, manipulamos a expressão convenientemente. Assim,

$$10 = 1 \cdot 6 + 4 \Rightarrow -10 = -1 \cdot 6 - 4.$$

Como $-10 = -1 \cdot 6 - 4 = -1 \cdot 6 - 4 + 6 - 6$, obtemos

$$\begin{aligned} 10 = 1 \cdot 6 + 4 \quad &\Rightarrow \quad -10 = -1 \cdot 6 - 4 \\ &\Rightarrow \quad -10 = -1 \cdot 6 - 4 + 6 - 6 \\ &\Rightarrow \quad -10 = 6 \cdot (-1 - 1) + 2 \\ &\Rightarrow \quad -10 = 6 \cdot (-2) + 2 \\ &\Rightarrow \quad q = -2 \quad \text{e} \quad r = 2. \end{aligned}$$

c) Sendo $a = -1243$ e $b = -4$, efetuamos a divisão de 1243 por 4 e usamos artifício análogo ao do caso 2. Temos:

$$\begin{aligned} 1243 = 310 \cdot 4 + 3 \quad &\Rightarrow \quad -1243 = 310 \cdot (-4) - 3 \\ &\Rightarrow \quad -1243 = 310 \cdot (-4) - 3 + 4 - 4 \\ &\Rightarrow \quad -1243 = -4 \cdot (310 + 1) + 1 \\ &\Rightarrow \quad -1243 = -4 \cdot 311 + 1 \\ &\Rightarrow \quad q = 311 \quad \text{e} \quad r = 1. \end{aligned}$$

♣

Proposio 1.6 *Sejam $a, b \in \mathbb{Z}$ com $b > 0$ e q o quociente da divisão de a por b. Então, $q = [\frac{a}{b}]$, ou seja, q é o maior inteiro menor ou igual a $\frac{a}{b}$.*

Demonstração: Como

$$a = bq + r,$$

com $0 \leq r < b$, segue que

$$\frac{a}{b} = q + \frac{r}{b},$$

sendo $\frac{r}{b} \in \mathbb{Q}$ tal que $0 \leq \frac{r}{b} < 1$. Por isso,

$$q \leq \frac{a}{b} = q + \frac{r}{b} < q + 1,$$

de maneira que $q = [\frac{a}{b}]$. ■

1.3.1 Máximo Divisor Comum

O conceito de máximo divisor comum tem estreita relação com subconjuntos $\mathbb{Z}$, tais como, os Ideais, que foram introduzidos com o objetivo de solucionar algumas questões em Teoria dos Números. Hoje em dia, seu estudo é realizado em Teoria dos Anéis.

Definio 1.3 *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Diz-se que $d \in \mathbb{N}$ é **máximo divisor comum** (mdc) entre a e b quando as seguintes condições são satisfeitas:*

(a) *$d \mid a$ e $d \mid b$.*

(b) *Se $c \mid a$ e $c \mid b$, então $c \mid d$.*

Em outras palavras, máximo divisor comum de a e b é um número natural que os divide e é divisível por todo divisor comum de a e b.

Observao 1.5 *Se $a = b = 0$, vamos acordar que o máximo divisor comum de a e b é 0.*

Nosso objetivo é provar que o natural d na condição acima existe e é único.

Propriedades

Lema 1.3 *Se os inteiros a e b têm um máximo divisor comum, então ele é único.*

Demonstração: Se d_1 e d_2 são máximos divisores comuns de a e b, então, por definição,

$$d_1 = \lambda_1 d_2 \quad \text{e} \quad d_2 = \lambda_2 d_1, \quad \text{com} \quad \lambda_1, \lambda_2 \in \mathbb{N}.$$

Substituindo o valor de $d_2 = \lambda_2 d_1$ em $d_1 = \lambda_1 d_2$, obtemos

$$d_1 = (\lambda_1 \lambda_2)\, d_1 \Rightarrow 1 = \lambda_1 \lambda_2 \Rightarrow \lambda_1 = \lambda_2 = 1.$$

Por conseguinte, $d_1 = d_2$. ♣

Dados dois inteiros a e b ambos não-nulos, vamos indicar por $mdc(a, b)$ o máximo divisor comum entre eles, quando este existir. Temos,

$$mdc(a, b) = mdc(-a, b) = mdc(-a, -b) = mdc(a, -b). \tag{1.2}$$

Além disso, se $a = 0$ e $b \neq 0$, então $mdc(0, b) = |b|$. Por isso, vamos assumir que a e b são sempre positivos.

O próximo teorema além de garantir a existência de mdc de dois inteiros, mostra que $mdc(a, b)$ é uma combinação muito proveitosa de a e b. Esta combinação não é única, por exemplo,

$$\begin{aligned} mdc(18, 4) \;=\; 2 \;&=\; 1 \cdot \mathbf{18} + (-4) \cdot \mathbf{4} \\ &=\; -1 \cdot \mathbf{18} + 5 \cdot \mathbf{4}. \end{aligned}$$

Teorema 1.5 *Para quaisquer números naturais a e b, existe $d = mdc(a, b)$. Além disso, existem $x_0, y_0 \in \mathbb{Z}$ tais que*

$$d = ax_0 + by_0, \tag{1.3}$$

Demonstração: Consideremos o conjunto

$$X = \{ax + by : x, y \in \mathbb{Z}\}.$$

Obviamente, existem em X elementos que são estritamente positivos. Por exemplo, para $x = y = 1$, obtemos $a \cdot 1 + b \cdot 1 = a + b > 0$ e $a + b \in X$. Seja W o subconjunto de X constituído pelos elementos de X estritamente positivos. Desse modo, pelo PBO, W possui menor elemento $d \in W$. Vamos mostrar que $d = mdc(a, b)$; como $d \in W$, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$d = ax_0 + by_0. \tag{1.4}$$

Usando o algoritmo da divisão com os elementos a e d, temos

$$a = dq + r, \quad \text{com} \quad 0 \leq r < d. \tag{1.5}$$

Substituindo o valor de d em (1.4) em (1.5), segue que

$$\begin{aligned} r &= a - dq = a - (ax_0 + by_0)q \\ &= a - aqx_0 - bqy_0. \end{aligned}$$

Daí,

$$r = a(1 - qx_0) + b(-qy_0) \Rightarrow r \in W.$$

Mas, sendo $r < d$, então, pela minimalidade de d, devemos necessariamente ter $r = 0$, isto é, $a = dq$, o que mostra que $d \mid a$. Similarmente, prova-se que d também divide b. Agora, se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$, então $a = c\lambda_1$ e $b = c\lambda_2$, com $\lambda_1, \lambda_2 \in \mathbb{Z}$. Como $d = ax_0 + by_0$,

$$d = (c\lambda_1)x_0 + (c\lambda_2)y_0 = c(\lambda_1 x_0 + \lambda_2 y_0) \Rightarrow c \mid b.$$

Portanto, $d = mdc(a, b)$. ■

A expressão em (1.3) é conhecida como **Identidade de Bézout** para os elementos a e b.

Quando os inteiros $a > 0$ e $b > 0$ são "pequenos", então determina-se $d = mdc(a, b)$ sem muitas dificuldades. Mas, como determinar d quando a e b são números consideravelmente grandes? Por exemplo, quanto vale $mdc(18594,)$? Não é razoável determinar os divisores positivos de $a = 18594$ e $b = 3882$ e verificar o maior entre os divisores comuns. Isso seria tedioso!

O Lema 1.4 mostra que o algoritmo da divisão poder ser usado para calcular $d = mdc(a, b)$, quaisquer que sejam os inteiros a e b. O mesmo implicará em um método (o algoritmo de Euclides) para determinar d, o qual consiste em divisões sucessivas.

Lema 1.4 *Sejam a e b inteiros, $b \neq 0$, e q e r o quociente e resto da divisão de a por b, respectivamente, ou seja,*

$$a = qb + r, \quad com \quad 0 \leq r < |b|. \tag{1.6}$$

Então, $mdc(a, b) = mdc(b, r)$.

Demonstração: Por (1.6), todo divisor de b e r é também divisor de a. Por outro lado, se $d \in \mathbb{N}$ é tal que $d \mid a$ e $d \mid b$, então, como $r = a - qb$, segue que $d \mid r$. Isto é suficiente para que se tenha $mdc(a, b) = mdc(b, r)$. ■

Portanto, pelo Lema 1.4, o problema de determinar $mdc(a, b)$ reduz-se a calcular $mdc(b, r)$.

Exemplo 1.5 *Determinar $d = mdc(1020, 284)$ e expressá-lo na forma do Teorema* 1.5.

Solução: Como $1020 > 284$, vamos usar o algoritmo da divisão, dividindo $a = 1020$ por $b = 284$. Assim,

$$\begin{aligned}
1020 = 3 \cdot 284 + 168 &\Rightarrow mdc(1020, 284) = mdc(284, 168),\\
284 = 1 \cdot 168 + 116 &\Rightarrow mdc(284, 168) = mdc(168, 116),\\
168 = 1 \cdot 116 + 52 &\Rightarrow mdc(168, 116) = mdc(116, 52),\\
116 = 2 \cdot 52 + 12 &\Rightarrow mdc(116, 52) = mdc(52, 12),\\
52 = 4 \cdot 12 + 4 &\Rightarrow mdc(52, 12) = mdc(12, 4),\\
12 = 3 \cdot 4 + 0 &\Rightarrow mdc(12, 4) = mdc(4, 0) = 4.
\end{aligned} \tag{1.7}$$

Portanto, $mdc(1020, 284) = 4$. Vamos encontrar $x_0, y_0 \in \mathbb{Z}$ tais que $4 = 1020 \cdot x_0 + 284 \cdot y_0$. Isso consistirá em isolar os restos não nulos das divisões de baixo para cima das igualdades em (1.7), substituindo-os sucessivamente. Logo,

$$\begin{aligned}
4 &= 52 - 4 \cdot 12 = 52 - 4 \cdot (116 - 2 \cdot 52) = 9 \cdot 52 - 4 \cdot 116\\
&= 9 \cdot (168 - 1 \cdot 116) - 4 \cdot 116 = 9 \cdot 168 - 13 \cdot 116\\
&= 9 \cdot 168 - 13 \cdot (284 - 1 \cdot 168) = 22 \cdot 168 - 13 \cdot 284\\
&= 22 \cdot (1020 - 3 \cdot 284) - 13 \cdot 284 = 22 \cdot 1020 - 79 \cdot 284.
\end{aligned}$$

Assim, $4 = 22 \cdot 1020 - 79 \cdot 284$; desse modo, podemos escolher $x_0 = 22$ e $y_0 = -79$. ♣

Dois inteiros a e b são ditos **primos entre si** ou **relativamente primos** quando $mdc(a, b) = 1$. Por exemplo, 8 e 3 são primos entre si, pois $mdc(8, 3) = 1$; já 18 e 4 não são, uma vez que $mdc(18, 4) = 2$.

Como consequências imediatas do Teorema 1.5, temos:

Corolrio 1.3 *Os inteiros a e b são relativamente primos se, e somente se, existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$.*

Corolrio 1.4 *Sejam $a, b, c \in \mathbb{Z}$. Mostrar que se $a \mid bc$ e $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração: Por hipótese, $bc = ak$ com $k \in \mathbb{Z}$. Além disso, pelo Corolário 1.3, existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$. Logo,

$$\begin{aligned}
1 = ax + by &\Rightarrow c = cax + cby\\
&\Rightarrow c = cax + aky\\
&\Rightarrow c = a(cx + ky)\\
&\Rightarrow a \mid c.
\end{aligned}$$

■

Corolrio 1.5 *Sejam $a, b \in \mathbb{Z}$ tais que $mdc(a, b) = 1$. Mostre que se $a \mid c$ e $b \mid c$, então $ab \mid c$.*

Demonstração: Como $a \mid c$ e $b \mid c$, então

$$c = a\lambda_1 \quad \text{e} \quad c = b\lambda_2, \quad \text{com} \quad \lambda_1, \lambda_2 \in \mathbb{Z}. \tag{1.8}$$

Por outro lado, sendo $mdc(a, b) = 1$, então existem $x, y \in \mathbb{Z}$ tais que

$$1 = ax + by \Rightarrow c = cax + cby.$$

Multiplicando a primeira igualdade de (1.8) por b e a segunda por a, obtemos

$$cb = ab\lambda_1 \quad \text{e} \quad ca = ab\lambda_2.$$

Substituindo esses valores em $c = cax + cby$,

$$\begin{aligned} c = cax + cby &\Rightarrow c = ab\lambda_2 x + ab\lambda_1 y \\ &\Rightarrow c = ab(\lambda_2 x + \lambda_1 y) \\ &\Rightarrow ab \mid c. \end{aligned}$$

■

Capítulo 2

Alguns Resultados sobre Números Primos

2.1 Breve histórico

A noção de um número primo não é recente em matemática. Os primeiros a entenderem a importância dos números primos foram os gregos antigos. Atribuím-se ao grego Pitágoras de Samos ($VI\ a.C.$) os primeiros estudos sobre os números primos a mais ou menos $530a.C.$. Apesar de não se ter registros de sua vida e seus trabalhos, documentos antigos de várias gerações após esse matemático citam suas ideias, entre elas a definição de um número primo.

Pitágoras foi uma das figuras mais influente e ao mesmo tempo uma das mais misteriosas da matemática. Muitos mitos e lendas surgiram sobre sua vida e por isso é muito difícil separar o que existiu de fato e o que foi inventado. Acredita-se que tenha feito muitas viagens pelo mundo antigo e nelas adquiriu muitas de suas habilidades matemáticas, estudando propriedades dos números e o relacionamento entre eles.

O livro mais antigo de matemática que chegou completo aos nossos dias foi uma coleção denominada "Elementos", escrito por volta de $350a.C.$ por Euclides de Alexandria ($300d.C.$), o primeiro gênio da matemática, que se sabe. "Elementos"é uma das obras matemáticas mais belas e mais reproduzidas no mundo ocidental. É considerado o livro-texto mais bem-sucedido de toda história da matemática. É formado por 13 volumes, que incluiam alguns resultados já conhecidos há muito tempo e de autorias não somente Euclides. Por ser tão completa, essa coleção era praticamente a única utilizada na época e sua influência permaneceu por mais de dois milênios. Considerado um dos maiores best sellers mundiais.

Euclides dedicou os volumes VII e IX a conceitos sobre Teoria dos Números. Suas ideias eram absolutamente compatíveis com as ideias de Pitágoras e bastante semelhante as atuais. Em "Elementos"encontra-se várias influências de Pitágoras. Por exemplo, o número 1 era chamado de unidade, da mesma forma na obra de Euclides.

Um número é definido como uma composição que se faz com as unidades, tanto por Pitágoras como por Euclides. Conceitos como "divide"era visto por eles como *"mede"*. Ou seja, dizer que 5 divide 10 é equivalente a dizer que 5 mede 10 ou seja, você pode enfileirar dois segmentos de 5 unidades de forma a obter o 10.

A definição de um número primo é dada na obra de Euclides, no volume VII da seguinte maneira:

"Protós arithmós estin monade mone metroymenos".

Ou seja, número primo é todo aquele que só pode ser medido através da unidade.

Na terminologia usada atualmente a expressão "medido por"traduz-se como "multíplo diferente dele próprio". Assim, número primo é aquele que é múltiplo apenas do 1, desconsiderando ele próprio. Assemelha-se bastante a definição que temos hoje.

"Um número inteiro $p > 1$ é primo se e somente se possui como divisores positivos apenas 1 e p".

Se $p > 1$ não é primo dizemos que p é composto, definição que também já se encontrava na obra de Euclides, como também uma demonstração de que a sequência dos números primos é infinita.

Uma observação importante é o fato de considerarmos $p > 1$. Como o único divisor de 1 é ele próprio, não se enquadra na definição de um número primo. Apesar de a obra não considerar também o 1 como sendo um número primo os motivos são diferentes e já vistos anteriormente. Além disso, por definição, o número 1 também não pode ser considerado um número composto. Ou seja, se p é um inteiro qualquer, então p é primo, é composto ou p é 1.

Pitágoras também teria observado que existem dois tipos de números, desconsiderando o número 1 que era apenas uma unidade: Os protoi arithmós (números primário ou primos) que são $2, 3, 5, 7$ e 11, por exemplo e os deuterói arithmós (números secundários) que são por exemplo o $4, 6, 8, 10$ e 12.

A importancia dos primos para a teoria dos números se equipara por muitos teóricos com os atómos na estrutura da matéria, podemos dizer que eles são os tijolos da construção numérica. Isso porque, conforme veremos, os números secundários, ou compostos, podem ser gerados a partir de produtos de primos, sendo portanto, esses últimos os números mais importantes da matemática. Mas, a importancia desses números não se limitam apenas à estrutura numérica. A forma como os números primos estão distribuidos parece totalmente desordenada, o que os torna ainda mais fascinantes, desde o tempo de Euclides, 2000 anos atrás. A partir disso, o que talvez fosse apenas uma preocupação de matemáticos, passa também a ser importante para a vitória britânica sobre o Nazismo alemão, para a invensão do computador, para a estrutura do sistema financeiro, para o estudo sobre o comportamento dos átomos, entre outros.

Muitos matemáticos, com certeza, passaram grande parte de suas vidas se dedicando ao estudo dos primos, porém ainda não se conhece a fundo esses números. Muitas vidas de dedicação, muitas hipóteses criadas mas, também muitas frustrações cercam esses elementos fundamentais da matemática.

2.2 Definições e Propriedades

Nesta seção vamos considerar alguns resultados básicos sobre números primos. Mais adiante, veremos outros que são obtidos de forma não elementar.

Definio 2.1 *Um número $p \in \mathbb{Z} - \{0, \pm 1\}$ diz-se **primo** quando seus únicos divisores positivos são 1 e $|p|$. Caso contrário, p é dito **composto**.*

Por exemplo, -3, 5 e 13 são primos, enquanto 9, 8 e 12 são compostos.

Observa-se que $a \in \mathbb{Z}$ composto significa dizer que

$$a = bc \quad \text{com} \quad 1 < b, c < |a| .$$

Além disso, p é primo se, e somente se, $-p$ é primo. Por isso, vamos considerar apenas primos positivos.

Proposio 2.1 (Euclides) *Sejam $a_1, a_2 \in \mathbb{Z}$ e p um número primo. Se $p \mid a_1 a_2$, então $p \mid a_1$ ou $p \mid a_2$.*

Demonstração: Se $p \nmid a_1$, então $mdc(a_1, p) = 1$, pois p é primo. Segue que $p \mid a_2$. ■

Por indução, para $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ e p primo,

$$p \mid a_1 a_2 \cdots a_n \Rightarrow p \mid a_i \tag{2.1}$$

para algum $i = 1, \ldots, n$. De fato, para $n = 1$, o resultado é imediato. Agora, suponhamos, por hipótese de indução, que o resultado seja válido para $n \geq 1$. Desse modo, para $a_1, a_2, \ldots, a_n, a_{n+1} \in \mathbb{Z}$, temos

$$\begin{aligned} p \mid a_1 a_2 \cdots a_n a_{n+1} &\Rightarrow p \mid (a_1 a_2 \cdots a_n)\, a_{n+1} \\ &\Rightarrow p \mid (a_1 a_2 \cdots a_n) \quad \text{ou} \quad p \mid a_{n+1}. \end{aligned}$$

Logo, por hipótese, $p \mid a_i$ para algum $i = 1, \ldots, n+1$.

Teorema 2.1 *Se $a > 1$, então existe um primo p tal que $p \mid a$.*

Demonstração: Consideremos o conjunto

$$W = \{a \in N : a > 1 \quad \text{e} \quad p \nmid a \quad \forall\ p \text{ primo}\}.$$

Se $W \neq \emptyset$, então pelo PBO, existe $d \in W$ com $d = \min W$. Como $d \mid d$, então d não pode ser primo. Por isso, $d = bc$ com $1 < b, c < n$. Desse modo, $b \notin W$, pois $d = \min W$. Por conseguinte, como $b > 1$, então deve existir um número primo p tal que $p \mid b$. Mas, como $b \mid p$, então $p \mid d$, isto é, $d \notin W$, o que é impossível. Essa contradição mostra que existe um primo p com $p \mid a$. ■

2.3 Teorema Fundamental da Aritmética

Como mencionado anteriormente, os números primos têm um papel fundamental na teoria dos números, conforme o Teorema Fundamental da Aritmética, que é considerado como um dos mais importantes resultados sobre primos.

Teorema 2.2 (Fundamental da Aritmética – TFA) *Todo número natural $a > 1$ pode ser escrito de forma única, a menos da ordem dos fatores, como produto de primos.*

Demonstração: Há duas coisas a serem demonstradas: a primeira é a existência dos primos; e a segunda é a unicidade da fatoração.
(**Existência**) Consideremos o conjunto

$$M = \{n \in \mathbb{N} : n \neq p_1 p_2 \cdots p_n\} \subset \mathbb{N},$$

para primos $p_1, p_2, \ldots, p_n$. Ou seja, M é constituído por todos os naturais que não são produtos de primos. Se mostrarmos que $M = \emptyset$, então a existência dos números primos estará provada. Suponhamos por absurdo que $M \neq \emptyset$; logo, pelo PBO, M possui um menor elemento $m \in M$. Dessa forma, m não pode ser primo e, por conseguinte, é composto. Assim, podemos escrevê-lo como

$$m = a \cdot b \quad \text{com} \quad 1 < a, b < m.$$

Como $a < m$ e $b < m$, então $a \notin M$ e $b \notin M$, pois $m = \min M$. Portanto, a e b são primos ou são produtos de primos. Logo, $m = a \cdot b$ é um produto de primos, o que é uma contradição.
(**Unicidade**) Suponhamos agora que

$$a = p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_m,$$

sendo $p_1, \ldots, p_n, q_1, \ldots, q_m$ são primos. Assim, por (2.1), temos que

$$p_1 \mid q_j$$

para algum $j = 1, \ldots, m$. Sem perda de generalidade, podemos supor que $p_1 \mid q_1$. Mas, como q_1 também é primo, então $p_1 = q_1$. Desse modo, pela lei do cancelamento, segue que

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Da mesma forma, temos $p_2 \mid q_j$ para algum $j = 2, \ldots, m$. Assumindo que $p_2 \mid q_2$, obtemos

$$p_3 \cdots p_n = q_3 \cdots q_m.$$

Continuando este processo, e assumindo que $n > m$, temos

$$1 = p_{m+1} \cdots p_n,$$

o que é impossível. Similarmente, se $n < m$, então

$$1 = p_{n+1} \cdots p_m,$$

o que também é impossível. Portanto, $m = n$ e $q_i = p_i$ para cada $i = 1, \ldots, n$. ■

Como os primos que surgem na fatoração de um dado $a \in \mathbb{N}$, $a > 1$, não são necessariamente distintos, temos:

Corolrio 2.1 *Todo número natural $a > 1$ pode ser escrito de forma única, a menos da ordem dos fatores, na forma*

$$a = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n},$$

em que $p_1 < p_2 < \cdots < p_n$ são números primos e $r_i \in \mathbb{N}$, para cada $i = 1, \ldots, n$. ■

Às vezes, se um dado primo p_k não surge com expoente maior do que zero na fatoração de $a \in \mathbb{N}$, $a > 1$, é conveniente escrever a na forma

$$a = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n} \cdot p_k^0.$$

Por isso, de uma forma geral, podemos considerar $r_i \in \mathbb{N} \cup \{0\}$, para cada $i = 1, \ldots, n$. Por este motivo, dados $a, b \in \mathbb{N}$, com $a > 1$ e $b > 1$, sempre é possível escrevê-los como

$$a = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n} \quad \text{e} \quad b = p_1^{s_1} \cdot p_2^{s_2} \cdots p_n^{s_n},$$

sendo $p_1, \ldots, p_n$ primos distintos e $r_i, s_i \in \mathbb{N} \cup \{0\}$.

Por exemplo, $a = 300 = 2^2 \times 3 \times 5^2$ e $b = 154 = 2 \times 7 \times 11$. Portanto,

$$a = 2^2 \cdot 3 \cdot 5^2 \cdot 7^0 \cdot 11^0 \quad \text{e} \quad b = 2 \cdot 3^0 \cdot 5^0 \cdot 7 \times 11.$$

2.3.1 Teste de Primalidade

Teorema 2.3 *Se $n > 1$ é composto, então n possui, necessariamente, um divisor primo p tal que $p \leq \sqrt{n}$.*

Demonstração: Sendo n um número composto, então

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

Se $a > \sqrt{n}$ e $b > \sqrt{n}$, então

$$n = b \cdot c > \sqrt{n} \cdot \sqrt{n} = n,$$

o que é impossível. Portanto, $a < \sqrt{n}$ ou $b < \sqrt{n}$, digamos que $1 < a < \sqrt{n}$. Pelo TFA, existe um primo p tal que $p \mid a$ $(p \leq a)$ e, por conseguinte, $p \mid n$. ■

Em outras palavras, o Teorema 2.3 nos mostra que, para verificarmos se um dado número $n > 1$ é primo, é suficiente verificarmos a divisibilidade pelos primos $p \leq \sqrt{n}$. O seguinte exemplo dá uma ilustração deste método.

Exemplo 2.1 *Para o número* $n = 103$,*temos que* $\sqrt{103} \leq 10$ *e os primos menores ou iguais a* 10 *são* $2, 3, 5$ e 7. *Como nenhum destes primos divide* n, *concluímos que* n *é primo.* ♣

O TFA trata-se da existência e unicidade da fatoração em primos de um dado $a \in \mathbb{N}$. Entretanto, sua demonstração não nos fornece um método de fatoração de a. Do ponto de vista computacional, a decomposição em fatores primos para inteiros relativamente grandes continua sem solução satisfatória.

2.3.2 Crivo de Eratóstenes

Eratóstenes $(276-194\ a.C.)$ nasceu em Cirene. Além de matemático, ele foi astrônomo, historiador, geográfo e filósofo grego. Tornou-se bibliotecário da Universidade de Alexandria com aproximadamente 40 anos de idade, convite feito pelo rei Ptolomeu III do Egito. Escreveu diversas obras, mas muitas delas foram perdidas. Morreu em Alexandria, 194 a.C.

Uma questão aparentemente simples sobre números primos é a de determinar, dentre os inteiros positivos, todos os números primos até certo número dado. Essa questão foi resolvida na antiguidade por Eratóstenes. Baseiando-se no Teorema 2.3 ele elaborou um método para determinar todos os números primos até um certo número inteiro n. O método consiste em escrever todos os números inteiros desde o número 2 até n. Depois suprimos todos os inteiros compostos múltiplos dos primos p tais que $p \leq \sqrt{n}$ (considerando apenas a parte inteira da raíz, com um arredondamento "para menos"). Esse processo funciona como uma "peneira"onde restam apenas os números primos menores que ou iguais n. Esse método ficou conhecido como o Crivo de Eratóstenes.

Exemplo 2.2 *Construir a tabela de números primos menores que 50.*

Solução: Como $\lfloor\sqrt{50}\rfloor = 7$, basta eliminar da tabela abaixo os números que são múltiplos dos primos menores ou iguais 7, ou seja,os múltiplos de 2, 3, 5, 7.

.	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50

Portanto, os números que restam são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 e 47. Sendo portanto, os primos menores que 50.

2.3.3 Fatoração de Fermat

Seja $a \in \mathbb{N}$ um número composto. Logo, podemos escrevê-lo na forma

$$a = 2^r \cdot b,$$

sendo b um inteiro ímpar e $r \in \mathbb{N} \cup \{0\}$. Se b for primo (isto pode ser verificado pelo Teorema 2.3), então a fatoração de a como produto de primos é $a = 2^r \cdot b$. Caso contrário, consideremos os seguintes passos:

Passo1 Seja $m = [\sqrt{b}]$, sendo $[\sqrt{b}]$ o maior inteiro menor ou igual a $\sqrt{b}$.

Passo2 Se $m^2 - b = n^2$, então $b = (m - n)(m + n)$.

Passo3 Se $m^2 - b \neq n^2$, então some 1 a m e volte ao passo 2.

Exemplo 2.3 *Obter a fatoração em potência de primos do número* $a = 2156$.

Solução: O número a não é primo, pois $2 \mid a$ e além disso, $a = 2^2 \cdot 539$, de modo que $r = 2$ e $b = 539$. Vamos encontrar apenas um fator primo de 539, pois os outros, caso existam, são obtidos similarmente. Consideremos $m = [\sqrt{539}] = 23$; logo

$$m^2 - b = 23^2 - 539 = -10 \neq n^2.$$

Somando 1 a 23,

$$(m + 1)^2 - b = 24^2 - 539 = 37 \neq n^2.$$

Somando 1 a 24,

$$25^2 - b = 25^2 - 539 = 86 \neq n^2.$$

Continuando este processo, somando 1 a 29 (pois antes de 29 não se encontra um quadrado perfeito), obtemos

$$30^2 - b = 30^2 - 539 = 361 = 19^2.$$

Desse modo,

$$\begin{aligned} 539 = 30^2 - 19^2 &= (30+19)(30-19) \\ &= 49 \cdot 11. \end{aligned}$$

Portanto, $539 = 49 \cdot 11 = 7^2 \cdot 11$. Consequentemente, $a = 2^2 \cdot 539 = 2^2 \cdot 7^2 \cdot 11$. Observa-se que a determinação do fator primo $p = 7$, implicou diretamente na determinação do fator $q = 11$. Isto naturalmente se deve ao fato de o número 539 ser relativamente pequeno. Entretanto, quando isso não ocorrer, o processo deve ser repetido até que se tenha todos os fatores primos de a. ♣

Apresentaremos a seguir algu| consequências do TFA, uma na forma de teorema e outras como exemplos.

2.4 A Sequência dos Números Primos

O teorema que segue deve-se a Euclides.

Teorema 2.4 *O conjunto dos números primos é infinito.*

Demonstração: Suponhamos por absurdo que o conjunto dos números primos seja finito. Sejam então $p_1, p_2, \ldots, p_n$ todos primos e consideremos $a \in \mathbb{N}$ dado pelo produto dos $p_{i,s}$ acrescido do número 1, isto é,

$$a = p_1 p_2 \cdots p_n + 1.$$

Como $a > p_i$ para todo $i = 1, \ldots, n$, então a não pode ser primo. Além disso, como o resto da Divisão Euclidiana de a por p_i é 1, então $p_i \nmid a$, ou seja, a não é divisível por nenhum dos primos $p_1, p_2, \ldots, p_n$. Desse modo, a não é primo nem é divisível por qualquer primo, o que contraria o TFA. ■

Exemplo 2.4 *Mostrar que $\sqrt{2}$ é irracional.*

Solução: Suponhamos que $\sqrt{2} \in \mathbb{Q}$, então podemos reescrevê-lo como sendo $\sqrt{2} = \frac{a}{b}$ com a e b primos entre si. Elevando ao quadrado ambos os lados de $\sqrt{2} = \frac{a}{b}$, obtemos

$$2 \cdot b^2 = a^2. \tag{2.2}$$

Como $a > 1$ e $b > 1$, então a^2 e b^2 têm em suas fatorações sempre um número par de primos (incluindo repetições). Assim, o lado esquerdo de (2.2) tem um número ímpar de primos, e seu lado direito tem um número par de primos. Isso contradiz o TFA. ♣

Exemplo 2.5 *Provar que se o polinômio*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

com $a_i \in \mathbb{Z}$ para $i = 1, \ldots, n$, é tal que $p(a) = 7$ para quatro valores de $a \in \mathbb{Z}$, então $p(a) \neq 14$ para qualquer $a \in \mathbb{Z}$.

Solução: Observa-se primeiramente que o número 7 pode ser fatorado em no máximo três diferentes fatores, $7 = (-1)\,(1)(-7)$. Por hipótese,

$$p(a_k) = 7, \qquad k = 1, 2, 3, 4$$

para distintos a_k. Assim, $p(a_k) - 7 = 0$, ou seja, $x - a_k \mid p(x) - 7$ Desse modo,

$$p(x) - 7 = (x - a_1)(x - a_2)(x - a_3)(x - a_4)q(x), \tag{2.3}$$

para algum polinômio $q(x)$ com coeficientes inteiros. Por absurdo, suponhamos que exista um inteiro n tal que $p(n) = 14$. Logo, por (2.3),

$$7 = p(n) - 7 = (n - a_1)(n - a_2)(n - a_3)(n - a_4)q(n).$$

Desde que os fatores $(n - a_k)$ são todos distintos, então decompomos o número 7 em pelo menos quatro fatores distintos o que, pelo TFA, é impossível. ♣

2.4.1 Distribuição dos números primos

Ao se observar uma lista de números primos a primeira impressão que se pode ter é que estão distribuidos de forma desordenada: às vezes aparecendo próximos uns dos outros, às vezes bastante afastados, enfim analisando pequenos grupos não se encontra regularidade nessa distribuição.

A forma com que os números primos estão distribuidos no conjunto dos números inteiros é tão irregular que do mesmo modo que podemos encontrar uma infinidade de números primos num determinado intervalo, em outro podemos obter apenas números compostos. Como veremos nos teoremas a seguir.

Teorema 2.5 *Para $n \geq 1$ podemos determinar n inteiros consecutivos tais que nenhum deles sejam primos.*

Demonstração: Consideremos a sequência

$$(n + 1)! + 2,\ (n + 1)! + 3,\ \ldots\ ,(n + 1)! + n + 1.$$

Observe que os elementos dessa sequência são da forma $(n + 1)! + k$, onde $2 < k \leq n + 1$. Além disso, $k \mid (n + 1)! + k$ segue que todos os números da sequência são compostos. ♣

Teorema 2.6 (Chebychev) *Dado um inteiro positivo n, existe sempre um número primo entre n e $2n$.*

Exemplo 2.6 *Para $n = 12$ teremos o intervalo entre 12 e 24. Neste intervalo temos os primos 13, 17, 19 e 23.*

Fazendo uma análise mais profunda foi que por volta de 1800 o matemático francês Adrien - Marie Legendre $(1752 - 1833)$ formulou uma conjectura que aparentemente define uma certa ordem em relação a distribuição do números primos, partindo da definição abaixo.

Definio 2.2 *Seja* $x \in \mathbb{Z}_+^*$. *Chamaremos de* $\pi(x)$ *a função que relaciona* x *com o número de primos inferiores ou iguais a ele próprio.*

Exemplo 2.7 *Os números primos menores ou iguais a* 20 *são* 2, 3, 5, 7, 11, 13, 17 *e* 19. *Assim,* $\pi(20) = 8$. *Do mesmo modo,* $\pi(100) = 25$ *e* $\pi(1000) = 168$.

No gráfico abaixo, podemos verificar que a função para valores pequenos de x não se comporta de forma regular.

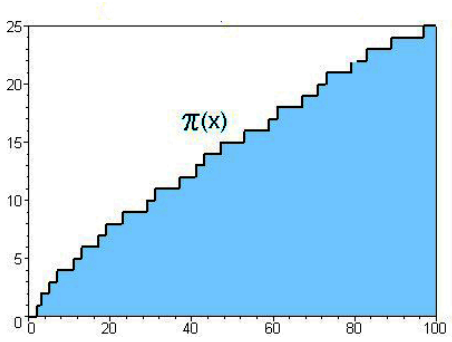

Figura 2.1: Gráfico da função $\pi(x)$ para valores de $x \leq 100$.

De fato, existe certa irregularidade. Mesmo assim, existe uma "tendência"ao que se parece bastante definida como podemos ver no próximo gráfico.

Dessa forma, essa tendência motivou diversos matemáticos na procura de uma função que se "assemelhe"a $\pi(x)$. Essa busca contribuiu bastante no que se refere ao estudo sobre os números primos. Um exemplo, dessa funções é a função Zeta de Riemann $(1826 - 1866)$. Riemann trabalhava nessa função quando percebeu uma relação existente com os números primos. Ele observou que os zeros dessa função tinham uma conexão com a forma com que os primos são distribuidos mas não sabia como demonstrar isso. Sua descoberta se equipara a primeira fórmula de Einstein, ela dava harmonia a distribuição dos números primos. Alguns matemáticos como por exemplo, G. H. Hardy $(1877 - 1947)$ e Srinivasa Ramanujan $(1887 - 1920)$ mostraram que essa hipótese de Riemann era verdadeira para uma infinidade de números primos. O

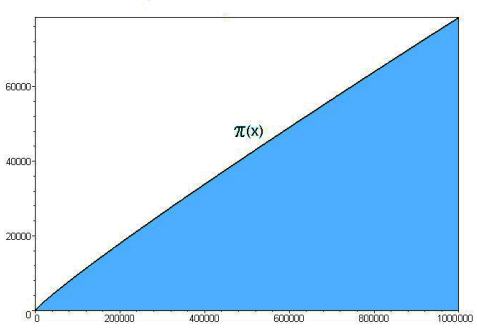

Figura 2.2: Gráfico da função $\pi(x)$ para valores de $x \leq 1000000$.

matemático Alan Turing (1912 − 1954), conhecido como o Pai da Ciência da Computação, trabalhou também na hipótese de Riemann. Construiu uma máquina que explorava o gráfico da função zeta em busca de zeros da função que pudessem tornar a hipótese falsa, não concluindo seu trabalho.

A hipótese é um poucos problemas não resolvidos do Programa de Hilbert (Proposta, feita em 1921 pelo matemático alemão David Hilbert, de reformular as bases da matemática de forma rigorosa, partindo da aritmética). É tão difícil que em 2000 o Clay Mathematics Institute ofereceu um prêmio de 1 milhão de dólares a quem prová-lo. Apesar de não ser objetivo desse trabalho detalhar sobre essa função, vale destacar aqui o gráfico da função Zeta de Reimann $\zeta(x)$ e o gráfico de $\pi(x)$.

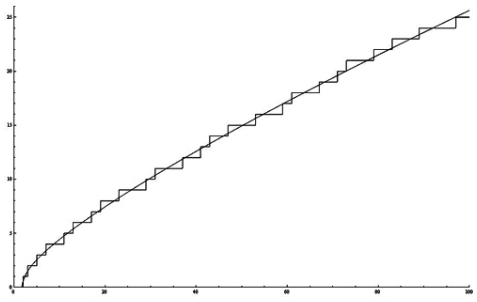

Figura 2.3: Representação de $\pi(x)$ e $\zeta(x)$.

Devido a irregualaridade da sequência dos números primos no conjunto dos números

inteiros positivos, muitas tentativas foram realizadas para encontrar alguma função $\pi(n)$ de modo a fornecer a sequência de números primos ou pelo menos fornecer somente primos quando n percorre os números inteiros. A próxima seção tratará de algumas dessas tentativas.

2.5 Fórmulas que geram números primos

2.5.1 Fórmula de Euler

Em 1772 Leonhard Euler $(1707 - 1783)$ descobriu o polinômio $f(n) = n^2 + n + 41$. Acreditava-se que $f(n)$ fosse sempre primos para cada, com $n \in \mathbb{N}$. Essa afirmação é verdadeira para os casos em que $n \leq 39$. Já para $n = 40$, $f(40)$ não é primo. De fato,

$$\begin{aligned} f(40) &= 40^2 + 40 + 41 \\ &= 40(40 + 1) + 41 \\ &= 40 \cdot 41 + 41 \\ &= 41(40 + 1) \\ &= 41^2. \end{aligned}$$

Apesar da facilidade em mostrar que essa afirmação é falsa para $n \in \mathbb{N}$, como na Idade Média ainda acreditava-se que ela fosse verdadeira? A resposta está na notação que temos hoje, o que simplifica os proble|. mama

2.5.2 Fórmula de Fermat

Consideremos

$$f(n) = 2^{2^n} + 1,\ n \in \mathbb{N}.$$

Para $n = \{1, 2, 3, 4\}$ obtemos $f(1) = 2^{2^1} + 1 = 5$, $f(2) = 2^{2^2} + 1 = 17$, $f(3) = 2^{2^3} + 1 = 257$, $f(4) = 2^{2^4} + 1 = 65537$. Onde todos são primos. Entretanto, Leonhard Euler mostrou um tempo depois que $f(5) = 2^{32} + 1 = 4294967297 = (641) \cdot (6700417)$ logo, $f(5)$ não é primo. O que nos mostra que essa conjectura também não é válida para todo $n \in \mathbb{N}$.

2.5.3 Fórmula de Mersenne

Mersenne $(1588 - 1648)$ afirmou que todo o número natural $M_p = 2^p - 1$ é primo para os primos $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, e é composto para todos os outros primos $p < 257$. Sabemos que essa afirmação é incorreta. De fato, $M_{67} = 267 - 1$ e $M_{257} = 2257 - p$ não são primos e mais, Mersenne ainda excluiu da sua lista $p = 61$, $p = 89$ e $p = 107$. Até 2008 eram conhecidos 47 primos de Mersenne, alguns deles muito

grandes como por exemplo: $230402457-1$, $232582657-1$, $237156667-1$, $242643801-1$, $243112609-1$, este último com 12978189 dígitos.

Muitas conjecturas apesar da linguagem simples ainda continuam sem solução. Veremos na próxima seção algumas delas.

2.5.4 Conjectura de Goldbach

Em 1742, Christian Goldbach $(1690-1764)$ escreveu uma carta a Euler sugerindo que *"todo inteiro $n > 5$ é soma de três primos"*. Em resposta, Euler observou que era equivalente dizer que *"todo inteiro par maior ou igual a 4 é soma de dois primos"*. Esta última ficou conhecida como Conjectura forte de Goldbach.

Georg Cantor $(1845-1918)$ verificou em 1894 a conjectura para todos os números pares inferiores a 1000. Em 1897, R. Haussner ampliou essa lista até 5000.

Em 2012 e em 2013, o matemático peruano Harald Andres Helfgott publicou dois trabalhos em quais afirma ter demonstrado a Conjectura fraca de Goldbach. A conjectura afirma que "*todo número ímpar maior que 5 pode ser expresso como soma de três números primos*". A prova está em análise e ainda vai demorar alguns meses para ser confirmada, de acordo com o próprio. Ele afirma também que essa pesquisa dificilmente contribuirá para comprovação da Conjectura forte de Goldbach. Acredita que a mesma "pode não ser resolvida nas nossas vidas".

2.5.5 Todo número ímpar $n > 5$ é soma de três primos

Em 1937, Vinogradov $(1891-1983)$ provou que essa conjectura é verdade para números suficientemente grandes. Borodzkin mostrou que é verdadeira para $n > 3^{14348907} = 3^{3^{15}}$. Em 1989, Chen e Wang reduziram esse limite para $n > 10^{43000}$. Mas, ainda é um valor muito grande para testar todos os menores que este, mesmo com o uso de computadores.

2.5.6 Existem infinitos pares de primos consecutivos

Chama-se primos consecutivos, ou **primos gêmeos** se a diferença entre eles for 2. Ou seja, serão ditos primos gêmeos se forem consecutivos na sequência de números primos.

Exemplo 2.8 *Temos que* 3 *e* 5*,* 5 *e* 7*,* 11 *e* 13, 17 *e* 19*,* 29 *e* 31*,* 41 *e* 43 *são pares de primos gêmos.*

Presumiu-se que há um número infinito de primos gêmeos, mas até hoje essa afirmação não foi provada. Em abril de 2013, o matemático Yitang Zhang chegou a um resultado profundo. Mostrou um número infinito de pares de primos cuja separação é menor que um limite superior finito 70 milhões. O maior par de primos gêmeos, até o momento, foi descoberto em dezembro de 2011 e tem 200700 dígitos, cada um.

2.5.7 Existe sempre um número primo entre n^2 e $(n+1)^2$

Entre 1 e 4 temos o 2 e o 3, por exemplo. Entre 4 e 9 temos o 5 e 7 entre 9 e 16 temos 11 e 13.

2.5.8 Existe infinitos primos da forma k^2+1

Por exemplo, $5 = 2^2 + 1$, $17 = 4^2 + 1$, $37 = 6^2 + 1$.

2.6 Alguns primos importantes

2.6.1 Primos de Sophie Germain

Um número primo p é dito Primo de Sophie Germain se $2p+1$ for também um número primo. Tornaram-se importantes e chamados assim depois que a matemática Sophie Germain provou o Teorema de Fermat ($x^n + y^n = z^n$ não tem solução em $\mathbb{Z}^*$ para $n > 2$) para expoentes divisíveis por esses primos. Por exemplo, $2, 3, 5, 11, 23, 29...$

2.6.2 Primos de Mersenne

Os números primos da forma $M_p = 2^p + 1$ com p sendo primo positivo são chamados de Primos de Mersenne. Eles foram o foco da maioria das primeiras pesquisas sobre grandes números primos. Por exemplo, $M_2 = 2^2 + 1$; $M_{19} = 2^{19} + 1$; $M_{57885161} = 2^{57885161} + 1$, este ultimo com 17.425.170 dígitos.

2.6.3 Primos de Fermat

Os primos da forma $F_n = 2^{2^n} + 1$ são chamados Números Primos de Fermat em homenagem a Pierre de Fermat $(1601 - 1655)$. Ele havia conjecturado que F_n era sempre um número primo, para todo $n \geqslant 0$. Entretanto, $F_5 = 2^{2^5} + 1$ é divisível por 641, portanto não é primo. São exemplos de Primos de Fermat, $F_0 = 2^{2^0} + 1$, $F_4 = 2^{2^4} + 1$.

Generalização de Fermat

A generalização dos números primos de Fermat é da forma $F_{b,n} = b^{2^n} + 1$, com $b > 1$ e $n > 0$. Por exemplo,

$$F_{689186,131072} = 689186^{131072} + 1 \quad \text{e} F_{475856,524288} = 475856^{524288} + 1,$$

este ultimo é o maior número dessa classe.

2.6.4 Primos Fatoriais

Os números primos fatoriais são da forma $n! \pm 1$. Como é o caso de $37! + 1$, $150209! + 1$ (712355 dígitos), $30! - 1$, $103040! - 1$ (471794 dígitos).

2.7 Maiores primos conhecidos

2.7.1 Antes dos computadores eletrônicos

O maior número primo encontrado através de cálculos manuais até o momento (e talvez possa continuar sendo para sempre) foi descoberto por Lucas ($1842 - 1891$) em 1876. O número encontrado por ele tem 39 dígitos.

Em 1951,o matemático Ferrier usou uma calculadora de mesa mecânica e algumas técnicas para encontrar um número primo maior que o encontrado por Lucas, este por sua vez tinha 44 dígitos.

Abaixo, segue uma tabela em ordem decrescente dos maiores números primos encontrados sem o uso de computadores eletrônicos, bem como o ano, a quantidade de dígitos e quem encontrou.

Número	**Dígitos**	**Ano**	**Matemático**
$2^{17} - 1$	6	1588	Cataldi
$2^{19} - 1$	6	1588	Cataldi
$2^{31} - 1$	10	1772	Euler
$\frac{2^{59}-1}{179951}$	13	1867	Landry
$2^{127} - 1$	39	1876	Lucas
$\frac{2^{148}+1}{17}$	44	1951	Ferrier

2.7.2 Com o advento dos computadores eletrônicos

Em 1951, Miller e Wheeler começaram a busca dos números primos sendo auxiliados pelos computadores eletrônicos.

No ano seguinte, Raphael Robinson ($1911 - 1995$) usando o CSAO (Standards Automatic Computer Ocidental) encontrando cinco novos Primos de Mersenne. A partir disso, com o aumento da velocidade dos computadores, Riesel ($1929-$) encontrou o M_{3217} usando uma máquina sueca Besk, entre outros listados abaixo.

Número	**Dígitos**	**Ano**	**Matemático**
$180 \cdot (M_{127})^2 + 1$	79	1951	Miller & Wheeler
M_{521}	157	1952	Robinson
M_{607}	183	1952	Robinson
M_{1279}	386	1952	Robinson
M_{2203}	664	1952	Robinson
M_{2281}	687	1952	Robinson
M_{3217}	969	1957	Riesel
M_{4423}	1332	1961	Hurwitz
M_{9689}	2917	1963	Gillies
M_{9941}	2993	1963	Gillies
M_{11213}	3376	1963	Gillies
⋮	⋮	⋮	⋮
$M_{3021377}$	909526	1998	Clarkson , Woltman , Kurowski , et al.
$M_{6972593}$	2098960	1999	Hajratwala , Woltman, Kurowski, et ai.
$M_{13466917}$	4053946	2001	Cameron , Woltman, Kurowski, et ai.
$M_{20996011}$	6320430	2003	Shafer , Woltman, Kurowski, et ai.
$M_{24036583}$	7235733	2004	Findley , Woltman, Kurowski, et ai.
$M_{25964951}$	7816230	2005	Nowak , Woltman, Kurowski, et ai.
$M_{30402457}$	9152052	2005	Cooper , Boone , Woltman, Kurowski, et ai.
$M_{32582657}$	9808358	2006	Cooper, Boone, Woltman, Kurowski, et ai.
$M_{43112609}$	12978189	2008	E_Smith , Woltman, Kurowski, et ai.
$M_{57885161}$	17425170	2013	Cooper, Woltman, Kurowski, et ai.

Observa-se que os maiores números primos, até o momento, são em sua maioria primos de Mersenne.

O maior número primo, até o momento, foi encontrado em janeiro de 2013 por Cooper, Woltman, Kurowsk entre outros, como parte do Great Internet Mersenne Prime Search (GIMPS), um projeto internacional que computação desenvolvido para encontrar números primos de Mersene.

A tabela completa está disponível em: <http://primes.utm.edu/notes/by_year.html#2>. Acesso em: 23 jun. 2013.

Bibliografia

[1] HARDY, G.H. e WRIGHT, E.M. – *An introduction to the theory of numbers (*4rd edition*)*, Oxford Claredon Press, 1968.

[2] SANTOS, JOSÉ PLÍNIO DE OLIVEIRA – *Introdução à Teoria dos Números (*2ª edição*)*, Rio de Janeiro: Instituto de Matemática Pura e Aplicada, CNPQ, 2000.

[3] MILIES, C. P. e COELHO, S. P. – *Números: Uma Introdução à Matemática (*3ª edição*),* Edusp, 2001.

[4] ALENCAR FILHO, EDGARD DE – *Teoria Elementar dos Números (*2ª edição*)*, São Paulo: Nobel, 1985.

[5] CALDWELL, Chris K.. The Prime Pages. Disponível em: <http://primes.utm.edu/>. Acesso em: 17 jun. 2013.

[6] D.E.JOYCE. *Euclid's Elements.* Disponível em: <http://aleph0.clarku.edu/˜djoyce/java/elements/elements.html>. Acesso em: 22 fev. 2012.

[7] BBC (Londres). The Music ¯of the Primes. Disponível em: <http://www.youtube.com/watch?v=f ybfr0zz-4>. Acesso em: 11 jun. 2012.

[8] THE NEW YORK TIMES (EUA). Solving a Riddle of Primes. Disponível em: <http://www.nytimes.com/2013/05/21/science/solving-a-riddle-of-primes.html>. Acesso em: 18 jun. 2013.

[9] HELFGOTT, Harald. About conjecutura weak Goldbach. [mensagem pessoal] Mensagem recebida por: <Isaedja de Andrade>. em: 21 jun. 2013.