UNIVERSIDADE ESTADUAL DA PARAÍBA - UEPB

CENTRO DE CIÊNCIAS HUMANAS E EXATAS - CCHE

CURSO DE ESPECIALIZAÇÃO EM MATEMÁTICA

Maria Aparecida Lopes

Introdução à Teoria dos Números e dos Números Primos

Monteiro - PB

2011

MARIA APARECIDA LOPES

Introdução à Teoria dos Números e dos Números Primos

Monografia apresentado ao Centro de Ciências Humanas e Exatas - CCHE da Universidade Estadual da Paraíba - UEPB , em cumprimento às exigências legais para a obtenção do título de Especialista no Curso de Especialização em Matemática. sob a orientação do Professor Ms. Luciano dos Santos Ferreira.

Monteiro - PB
2011

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA SETORIAL–CAMPUS VI

L864i LOPES, Maria Aparecida.

Introdução à Teoria dos Números e dos Números Primos /Maria Aparecida Lopes. – 2011.

36f.

Digitado.

Monografia (Especialização em Matemática) – Universidade Estadual da Paraíba, Centro de Ciências Humanas e Exatas, 2011.

"Orientação: Profº Me. Luciano dos Santos Ferreira, Universidade Estadual da Paraíba, Campus VI.

1 Números Primos 2. Equações Diofantinas 3. Tipos de Números Primos I. Título.

21. ed. CDD 512.72

MARIA APARECIDA LOPES

Introdução à Teoria dos Números e dos Números Primos

Monografia apresentado ao Centro de Ciências Humanas e Exatas - CCHE da Universidade Estadual da Paraíba - UEPB , em cumprimento às exigências legais para a obtenção do título de Especialista (em Matemática).

Aprovado pela banca examinadora em 28 de Setembro de 2011.

Banca Examinadora

Prof. Ms.Luciano dos Santos Ferreira
Centro de Ciências Humanas e Exatas- CCHE/UEPB

Prof. Ms. Luiz Lima de Oliveira Juniior
Dpto. Matemática - CCT/UEPB
EXAMINADOR

Prof. Ms. Joselma Soares dos Santos
Centro de Ciências Humanas e Exatas- CCHE/UEPB

Dedico este trabalho aos meus pais (in memorian) e ao grande amigo Don Egídio Bisol (hoje Bispo Diocesano de Afogados da Ingazeira.) A minha familia, pelo esforço dedicação e compreensão em todos os momentos da minha vida.

Agradecimentos

À Deus pela vida.
Aos meus queridos pais (in memorian) pelo grande amor dado a mim em todos os momentos bons e ruins, sempre me incentivaram nos estudos e me deram "colo"em minha caminhada.
Especialmente, ao professor Ms. Luciano dos Santos Ferreira, que de modo competente, calmo e marcado pelo diálogo e respeito, acreditou e conduzio a orientação deste trabalho.
Aos professores Ms. Luiz Lima de Oliveira Junior e Joselma Soares dos Santos, que aceitaram participar da banca examinadora, contribuiram de modo significativo para a conclusão deste trabalho.
À coordenação e ao corpo docente do curso de especialização, pelas contribuições, convívio, apoio e compreensão que contribuiram para minha formação de especialista.
À Don Egídio Bisol, hoje bispo da diocese de Afogados da Ingazeira, meu grande amigo e orientador espiritual, sempre esteve presente no meu dia-a-dia, com quem compartilho meus idéais e projetos.
À professora Ms. Thiciany Matsudo Iwano, competente, incentivadora e amiga.
Aos professores Ms. Roger Ruben Huaman Huanca, pela disponibilidade, compreenção e dedicação em sua nobre função de professor.
A todos os meus familiares, colegas de trabalho e da especialização, de forma especial a professora Solange Alves e Genilda Beliz que sempre estiveram do meu lado, incentivando-me na busca pelo conhecimento.
Ao professor Rônero Márcio Cordeiro Domingos, pela ajuda na digitação com o Latex, meu agradecimento especial.

Resumo

A teoria dos números é a ciência na qual se estudam propriedades e relações entre os números. Esta é uma área da matemática muito antiga, cujo desenvolvimento como todas as outras partes da ciência, segundo Gauss é rainha da matemática. O objetivo deste trabalho é fazer um breve relato histórico da "Teoria dos Números"e "Números Primos"com um estudo introdutório sobre alguns tópicos de números primos e divisibilidade. Mostraremos propriedades dos inteiros, bem como critérios de divisibilidade, propriedades de máximo divisor comum e mínimo múltiplo comum e demonstrações dos mesmos. Apresentaremos o algoritmo da divisão (Teorema 1.3) que é um dos resultados relevantes sobre a existência e unicidade do quociente e do resto na divisão de inteiros. Usamos o principio de indução matemática para estabelecer um resultado sobre os números inteiros. Destacamos as equações Diofantina, números primos e o importantissimo algoritimo "Crivo de Eratóstenes". Introduzimos os primos gêmeos e a conjectura de Goldbach e por fim trabalhamos alguns tipos especiais de números primos com respectivo exemplos e tabelas. A metodologia utilizada na realização deste trabalho tem como referencial a compreensão e a apresentação de resultados teóricos e demonstrações.

Palavras-Chave: Números Primos, Equações Diofantinas, Tipos de Números Primos.

Abstract

The theory of numbers is the science where the properties and relations between numbers is studied. It´s a very old area of mathematics and, since it´s related to all other parts of the science, Gauss calls it "the queen of mathematics". The objective of this study is to make a brief history of "Theory of Numbers"and "Prime numbers", with an introductory study of some aspects of prime numbers and their ability to divide. It shows the properties of the whole numbers, the criteria for division, properties of the greatest common divisor and the least common multiple and demonstrations of these. Furthermore, this study presents the algorithm of division (Theorem 1.3) which is one of the relevant results related to the existence and oneness of the quotient and the rest in division of whole numbers. It uses the principle of mathematic induction to establish a result on whole numbers. It emphasizes the Diofantina equation, prime numbers and the very important algorithm "Sieve of Eratosthenes". It introduces the twin primes and the Goldbach hypothesis and, finally, it works on some special types of prime numbers with their respective examples and boards. The methodology used in this study has its reference in the comprehension and presentation of theoretical results and demonstrations.

Keywords: Prime numbers, Diofantina equations, types of prime numbers.

Lista de Tabelas

Sumário

Introdução

A teoria dos números é uma ciência que têm como objetivo explicar a origem dos números, as relações entre eles e suas propriedades. O estudo das propriedades dos números inteiros positivos é o objetivo central da teoria dos números. Este trabalho é resultado de estudos realizados sobre "Números Primos". Os resultados aqui apresentados limita-se à parte elementar, onde estão apresentadas provas elementares de alguns teoremas e proposições.

Introduziremos os conceitos atráves de um significativo número de exemplos, procurando, desta forma, motivar estudos na área de teoria dos números. Vale mencionar aqui que, em teoria dos números, esta tarefa não é intrigante, pois é grande o número de problemas interessantes que não requerem ferramentas sofisticadas para sua compreenção.

Fornecemos, a seguir, uma breve descrição de cada capítulo.

No capítulo I, uma breve história da teoria do números e dos números primos. Estudamos propriedades elementares sobre divisibilidade no conjunto dos inteiros, sendo o algoritimo da divisão (teorema 1.3) resultado mais importante, sobre a existência e a unicidade do quociente e do resto na divisão de inteiros. Também usamos o principio de indução matemática para determinar resultado sobre os números inteiros, dentre elas o estudo de máximo divisor comum e mínimo multiplo comum entre inteiros não nulos.

Apresentaremos o importantíssimo conceito das equações diofantinas do célebre matemático grego Diofanto de Alexandria (-250d.C) e exemplos.

No capítulo II, forneceremos alguns resultados clássicos sobre os números primos e o Teorema Fundamental da Aritmétrica (teorema 2.2) sobre a unicidade da representação de um inteiro como produto de potências de primos.

Uma das várias provas da existência de infinitos primos é apresentado no teorema (2.5) (Euclides).

Mostraremos um resultado que tem uma importante aplicação prática, para tentarmos provar se um número é primo. Este processo é chamado "CRIVO DE ERATOSTENES", hoje chamado de algorítmo.

Relembraremos no capitulo II, a importantíssima "CONJECTURA DE GOLDBACH", do século XVIII.

Terminaremos este capítulo com um estudo de tipos especiais de números primos que são os seguintes:

I) Números Primos Primordial
II) Números Primos Fatoriais
III) Números Primos Titânicos
IV)Números Primos Mersenne
V) Números Primos Fermat
VI)Números Primos Wilson
VII)Números Primos Wall-Sun-Sun
VIII)Números Primos Smarandache-Well
IX)Números Primos Wieferich
X)Números Primos Truncáveis
XI)Números Primos Sphie Germain
XII)Números primos de Fibonacci.

1 Contexto Histórico sobre a Teoria dos Números

1.1 História da Teoria dos Números

A teoria dos números é uma área da matemática que estuda as propriedades dos inteiros e a mesma é atestada nas civilizações mais antigas. Entretanto, é na Grécia que primeiro identificamos a teoria dos números, como assim entendemos até hoje. No que diz respeito aos inteiros, os gregos diferenciavam com a arte de calcular e a aritmética, ou estudo das propriedades fundamentais dos inteiros. A teoria dos números é herdeira da aritmética dos gregos. Entre os problemas da teoria dos números abordados pelos gregos antigos estão:

- O cálculo do máximo divisor comum entre dois números;
- A determinação dos números primos menores que um inteiro dado;
- A demonstração de que há uma infinidade de números primos.

Estes problemas são discutidos em detalhes num dos mais famosos livros de matemática, "Os Elementos"escrito pelo matemático Euclides, que viveu em Alexandria por volta de 300 a.C.

Vários outros matemáticos gregos estudaram os problemas da teoria dos números. Destes um dos mais importantes foi sem dúvida Diofante. Sua aritmética, escrita por volta de 250 d.C, trata principalmente da resolução de equações indeterminadas com coeficiente inteiros.

Embora a matemática tenha sido intensamente estudada por outros autores gregos, e, posteriormente, por árabes, indianos e europeus, a teoria dos números caiu em esquecimento até o século XVII.

Bachet, em 1612, publicou o texto original em grego da Aritmética de Diofante, incluindo uma tradução latina, que era a língua usada pelos europeus da época. Em algum momento entre 1621 e 1636, o francês Pierre de Fermat, magistrado da corte de Toulouse, adquiriu uma cópia desse livro. Fermat leu o texto de Diofante, anotando na margem as idéias que lhe ocorriam. Isso marcou o início de seu interesse pela teoria dos números, que posteriormente, expressou uma torrente de resultados importantes.

Na verdade, poucas pessoas exerciam a matemática como profissão naquela época. Pois, a comunicação entre os matemáticos também era precária, não havia revistas especializadas.

A comunicação era conduzida, principalmente, através de cartas e por algumas pessoas que serviam de “centros divisores” dos novos resultados. A primeira revista dedicada a matemática só foi criada em 1794.

Os mais famoso divulgador dos resultados obtidos da matemática foi o frade francês Marin Mersenne. Muito amigo de alguns dos maiores matemáticos da época, como Descartes, Pascal e o próprio Fermat. Foi na forma de cartas enviadas a Mersenne e a outros matemáticos contemporâneos que boa parte da obra de Fermat ficou conhecida. Depois de sua morte, em 1665, coube a Samuel Fermat seu filho, coletar e publicar a obra de seu pai, dispersa em cartas a anotações. Ele começou com a publicação da Aritmética de Diofante, incluindo todas anotações feitas por Fermat. Dessas anotações, a mais famosa é chamado o Último Teorema de Fermat: não existe solução não nula para equação $x^n + y^n = z^n$, onde n é maior ou igual a 3 e x, y, z números inteiros. Esse resultado só foi provado em 1995, pelo inglês Andrew Wiles, mais de 300 anos após ser enunciado por Fermat. O verdadeiro sucessor de Fermat foi o suíço Leonhard Euler, que nasceu em 1707, quarenta e dois dias após o falecimento de Fermat. Euler publicou uma obra imensa, tendo contribuído para quase todas as áreas da matemática pura e aplicada existentes no século XVIII. O interesse de Euler em Teoria dos Números teve início em sua correspondência com Cristian Goldbach, foi através dele que ele chegou à obra de Fermat.

A famosa conjectura de Goldbach que afirma, "Todo número par, maior que dois pode ser descomposto na soma de dois números primos". Esse resultado não foi provado até os dias de hoje. Porém, o desenvolvimento sistemático da teoria dos números, só iniciou com a obra as Disguisitiones Arithméticx, do alemão C.F.Gauss publicado em 1801. Em Teoria dos números é possível enumerar diversos resultados importantes (é usados até hoje) atribuídos a ele, como os números primos, números de Fibonnaci e congruência.

1.2 História dos Números Primos

Os primeiros números primos, bem como suas propriedades, foram pela primeira vez estudados intensamente pelos antigos matemáticos gregos. No papiro de Rhindi, por exemplo, há indícios de que o antigo povo egípcio tinha algum conhecimento sobre os números primos. No entanto, o registro mais antigo de um estudo explícito sobre números primos é devido aos gregos.

Pitágoras de Samos foi um dos percussores desse estudo, embora o seu interesse mais direcionado para o místico, chegando a criar a escola Pitagórica (500 a 300 a.c). Os grandes seguidores da época entendiam a idéia de primalidade, revelavam interesses em números perfeitos e amigáveis. A escola dava uma grande importância ao número ”1”, que era chamado de unidade. Os outros números tinham uma importância reduzida, pois todos eles representavam apenas multiplicidades da unidade e por isso eram chamados de números.

A partir dessas denominações, os pitagóricos começaram a perceber que existiam dois tipos de número: Números primos: são números que não podem ser gerados pela multiplicação, a partir de outros números, como $2, 3, 5, 7, 11$, e etc.

Números compostos ou secundários: são números que podem ser gerados a partir de outros números, como o $6 = 2.3$; $9 = 3.3$, ...

NO livro "Os elementos", Euclides prova que existem infinitos números primos. Está é uma das primeiras demonstrações conhecidas a usar o método da contradição, com à obtenção de um resultado. Os elementos de Euclides (cerca de 300 a.C), contém teoremas importantíssimos sobre os números primos, incluindo a demonstração de sua infinitude e o teorema fundamental da aritmética. Euclides também mostrou como construir um número perfeito a partir de um primo de Mersenne. Ao grego Eratóstenes, atribuiu-se um método simples para o cálculo de números primos, conhecido atualmente como crivo de Eratóstenes. Por outro lado, nos tempos atuais, os grandes números primos são encontrados por computadores, através de testes de primalidade mais complexos, como por exemplo o teste de primalidade AKS.

Fermat no início do século XVII, provocando a conjectura de Albert Girard, cria alguns teoremas que mais tarde seriam usados como base de muitos resultados em Teoria dos Números e de métodos para testes de primalidade que são utilizados até hoje. Fermat correspondeu-se com outros matemáticos do seu tempo, como Marim Mersenne, que junto com Fermat, formularam os números de Mersenne (número da forma $2^n - 1$).

Provar que um número é primo (para números com vários dígitos) não é feito pela divisão trivial. Vários matemáticos trabalharam em vários testes de primalidade para grandes números, ou seja, foi trabalhado especificamente alguns testes de primalidade como: AKS, Fermat, Lucas-Lehmer e outros, mesmo com a existência de vários testes de primalidade, nenhum deles funciona de forma rápida e eficaz.

Na era dos computadores e intensas pesquisas realizadas em busca de números primos, o maior primo conhecido é um primo de Mersenne.

1.3 Conceitos Fundamentais da Teoria dos Números

Veremos alguns conceitos básicos da Teoria dos Números necessários para o próximo capítulo.

1.3.1 Princípio de Indução Matemática

O princípio de indução matemática serve para provar proposições que dependem de n, um inteiro não negativo, que varia num subconjunto de $\mathbb{Z}$.

Esse princípio está baseado no seguinte axioma.

Princípio da Boa Ordenação

Todo subconjunto não vazio A de inteiros não negativos possui um elemento mínimo (isto é, existe $n_0 \in A$ tal que $n_0 \leq n$, para todo $n \in A$).

Princípio 1.1.1 (Indução Matemática - 1ª forma) Seja $\mathbb{N} = \{n_0, n_1, n_2, ...\}$ um conjunto de inteiros não negativos (suponha também $n_0 < n_1 < n_2 < ...$) e seja $S(n)$ uma proposição que depende de $n \in \mathbb{N}$, tal que:

(i) $S(n)$ é verdadeiro;

(ii) Se $m \in \mathbb{N}$ e $S(n)$ é verdadeiro para qualquer $n \in \mathbb{N}$ tal que $n < m$, então $S(m)$ é verdadeiro.

Então $S(n)$ é verdadeiro para todo $n \in \mathbb{N}$.

Prova.

Considere $F = \{l \in \mathbb{N} : S(l) \text{ não é verdadeiro}\}$. Suponha por absurdo que $F \neq \emptyset$. Então, pelo princípio da boa ordenação existe $l_0 \in F$, $l_0 > n_0$, tal que $l_0 \leq l$, para todo $l \in F$ (isto é, l_0 é um elemento minímo de F). Isto nos diz que $S(n)$ é verdadeiro para todo $n \in \mathbb{N}$ tal que $n < l_0$. Pela hipótese (b) temos que $S(l_0)$ é verdadeiro, uma contradição. Assim devemos ter $F = \emptyset$ e $S(n)$ verdadeiro para todo $n \in \mathbb{N}$. ■

Princípio 1.1.2 (Indução Matemática - 2ª forma) Sejam $N_0 = \mathbb{N} \cup \{0\}$ e $S(n)$ uma proposição que depende de $n \in N_0$, tal que:

(i) $S(0)$ é verdadeira;

(ii) Para cada $n \in N_0$, o fato de $S(n)$ ser verdadeiro implica $S(n+1)$ também ser verdadeira.

Portanto, $S(n)$ é verdadeira para qualquer $n \in N_0$.

Prova. A demonstração é completamente análoga à do princípio 1.1.1. ■

Exemplo 1.1. *Seja $S(n)$ a soma dos n primeiros inteiros positivos, então*

$$1+2+\ldots+n = \frac{n(n+1)}{2}.$$

Vamos utilizar o princípio 1.1.2. Note que o fato $S(1)$ é verdadeiro, pois $1 = \frac{1(1+1)}{2}$. Iremos mostrar que o fato de $S(n)$ ser verdadeiro faz com que $S(n+1)$, também o seja. Com efeito

$$1+2+\ldots+n+(n+1) = (1+2+\ldots+n)+(n+1)$$

$$= \frac{n(n+1)}{2} + (n+1)$$

$$= \frac{n(n+1)+2(n+1)}{2}$$

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

Logo, $S(n+1)$, é verdadeiro.

1.3.2 Teoria de Divisibilidade nos Números Inteiros

Um dos conceitos mais básicos da teoria dos números é o conceito da divisibilidade. Diz-se que a divide b, ou a é um divisor de b, ou ainda que b é múltiplo a se existe algum inteiro m no qual $b = am$. Na notação ultiliza-se $a \mid b$. Se a não divide b, então se escreve: $a \nmid b$.

Proposição 1.1. *Se a, b e c são inteiros $a \mid b$ e $b \mid c$, então $a \mid c$.*

Prova. Como $a \mid b$ e $b \mid c$, existem inteiros K_1 e K_2 com $b = K_1 a$ e $c = K_2 b$. Logo $c = K_2 K_1 a$ o que implica $a \mid c$. ■

Exemplo 1.2. *Como* $3 \mid 12$ *e* $12 \mid 48$*, então* $3 \mid 48$.

Proposição 1.2. *Se a, b, c, m e n são inteiros, c divide a e c divide b então c divide $(ma+nb)$.*

Prova. Se $c \mid a$ e $c \mid b$ então $a = K_1 c$ e $b = K_2 c$. Multiplicando-se estas duas equações respectivamente por m e n teremos $ma = mK_1 c$ e $nb = nK_2 c$. Somando-se membro a membro obtemos $ma + nb = (mK_1 + nK_2)c$, o que nos afirma que $c \mid (ma+nb)$. ■

Exemplo 1.3. *Como* $3 \mid 15$ *e* $3 \mid 42$*, então* $3 \mid (8.15 - 7.42)$.

Teorema 1.3. *A divisão tem as seguintes propriedades: Para todos os números a, d e $n \in \mathbb{Z}$ valem*

(i) $n|n$
(ii) $d|n \Rightarrow ad|an$
(iii) $ad|an$ *e* $a \neq 0 \Rightarrow d|n$.
(iv) $1|n$
(v) $n|0$.
(vi) $d|n$ *e* $n \neq 0 \Rightarrow |d| \leq |n|$.
(vii) $d|n$ *e* $n|d \Rightarrow |d| = |n|$.
$(viii)$ $d|n$ *e* $d \neq 0 \Rightarrow (n/d)|n$.

Prova. (i) Como $n = n \cdot 1$ segue da definição que $n|n$, inclusive para $n = 0$.
(ii) Se $d|n$ então $n = cd$ para algum inteiro c. Logo, $an = cad$ o que conclui a prova.
(iii) Se $d|n$ então $n = K_1 d$ e portanto n/d é um inteiro. Como $(n/d) \cdot d = n$ segue da definição que $(n/d)|n$. Os outros itens são consequência imediata da definição. ■

1.4 Algoritmo da Divisão

O algoritmo da divisão define precisamente o quociente e o resto da divisão de dois inteiros, mostra também que eles existem e são únicos.

Teorema 1.4. *Dados dois inteiros a e b, $b > 0$, existe um único par de inteiros q e r tais que $a = q.b + r$, onde $0 \leq r < b$. O inteiro q é chamado quociente e r é o resto da divisão de a por b. Observe que se b é divisor de a, então o resto é 0 e $a = q.b$*

Prova. Pelo teorema de Eudoxius com $b > 0$, existe q tal que $q.b \leq a < (q+1).b$. Subtraindo $q.b$, temos

$$q.b - q.b \leq a - q.b < (q+1).b - q.b$$

$$0 \leq a - q.b < b$$

fazendo $r = a - q.b$, então:

$$0 \leq r < b \ e \ r = a - q.b \Rightarrow a = q.b + r$$

Assim foi demonstrada a existência do quociente e do resto.Veja agora a demonstração da unicidade de q e r: Suponhamos que existe r_1 e q_1 são inteiros tais que

$$a = q_1.b + r_1,$$

temos

$$(qb + r) - (q_1.b + r_1) = 0$$

$$(q - q_1).b = (r_1 - r).$$

Então

$$b \mid (r_1 - r) \ (b \ divide \ (r_1 - r))$$

Como $r_1 < b$ e $r < b$, segue que $|r_1 - r| < b$. Concluímos que

$$r_1 - r = 0 \Rightarrow r_1 = r \quad \text{e} \quad (q - q_1).b = 0$$

Logo, $qb = q_1 b \Rightarrow q = q_1$ ■

Exemplo 1.4. $34/7$, *tem quociente* 4 *e resto* $6 \Rightarrow 34 = 4.7 + 6$
$25/3$, *tem quociente* 8 *e resto* $1 \Rightarrow 25 = 3.8 + 1$
$15/-4$, *tem quociente* -3 *e resto* $3 \Rightarrow 15 = (-3).(-4) + 3$

Exemplo 1.5. *Achar o quociente q e o resto r na divisão de $a = 59$ por $b = -14$ que satisfazem as condições do algoritmo da divisão.*

Efetuando a divisão usual dos valores absolutos de a e b. Obtemos:

$$59 = 14.4 + 3 \Rightarrow 59 = (-14).(-4) + 3 \ e \ 0 \leq 3 < |-14|$$

Logo, o quociente é $q = -4$ e o resto $r = 3$.

Exemplo 1.6. *Achar o quociente q e o resto r na divisão de $a = -79$ por $b = 11$ que satisfazem às condições do algoritmo da divisão.*

Efetuando a divisão usual dos valores absolutos de a e b, obtemos:

$$79 = 11.7 + 2$$

o que torna possível.

$$-79 = 11(-7) - 2.$$

Como o termo $r = -2 < 0$ *não satisfaz à condição* $0 \leq r < 11$*, somando e subtraindo o valor* 11 *de b ao segundo membro da igualdade anterior, temos:*

$$-79 = 11(-7) - 11 + 11 - 2 = 11(-8) + 9 \; com \; 0 \leq 9 < 11.$$

Logo, o quociente é $q = -8$ *e o resto* $r = 9$.

1.5 Máximo Divisor Comum de Dois Números.

Definição 1.5. *Sejam* $a, b \in \mathbb{Z}$ *dois números pelo menos um deles é diferente de zero, denotado por* $MDC(a,b)$ *é o maior inteiro que divide a e b, ou seja,*

(i) $d \mid a$ *e* $d \mid b$ *(d é divisor comum de a e b)*

(ii) *Se algum* $c \in \mathbb{N}$ *dividir ambos a e b então temos também* $c \mid d$.

Teorema 1.6. *Seja d o máximo divisor comum de a e b, então existem inteiros* n_0 *e* m_0 *tais que* $d = n_0 a + m_0 b$.

Prova. Seja B o conjunto de todas as combinações lineares $(na + mb)$ onde n e m são inteiros. Vamos escolher n_0 e m_0 tais que $c = n_0 a + m_0 b$ seja o menor inteiro positivo pertencente ao conjunto B. Iremos provar que $c \mid a$ e $c \mid b$.
Por contradição, suponhamos que $c \nmid a$. Então, pelo teorema 1.3, existem q e r tais que

$$a = q.c + r \text{ com } 0 < r < c.$$

Portanto, $r = a - qc = a - q(n_0 a + m_0 b) = (1 - qn_0)a + (-qm_0)b$. Isto mostra que $r \in B$, pois $(1 - qn_0)$ e $(-qm_0)$ são inteiros, o que é uma contradição, uma vez que $0 < r < c$ e c é o menor elemento positivo de B.

Logo, $c \mid a$ e de forma analóga se prova que $c \mid b$. Como d é divisor comum de a e b, existem inteiros K_1 e K_2 tais que $a = K_1 d$ e $b = K_2 d$ e, portanto, $c = n_0 a + m_0 b = n_0 K_1 d + m_0 K_2 d = d(n_0 K + m_0 K_2)$ o que implica $d \mid c$.

Do Teorema 1.3 (vi), temos que $d \leq c$ (positivos) e como $d < c$ não é possível, uma vez que d é máximo divisor comum. Logo, $d = c$. ■

Proposição 1.7. *Para todo inteiro positivo* t, $MDC(ta,tb) = tMDC(a,b)$.

Prova. Pelo Teorema 1.6 $MDC(ta,tb)$ é o menor valor positivo de $mta + ntb$ (m e n inteiros), que é igual a t vezes o menor valor positivo de $ma + nb = t.MDC(a,b)$. ■

Proposição 1.8. *Se $c > 0$ e a e b são divisíveis por c então*

$$MDC\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} MDC(a,b)$$

Prova. Como a e b são divisíveis por c, temos que $a \mid c$ e $b \mid c$ são inteiros. Basta então, substituir na proposição 1.7 "a"por $a \mid c$ e b por $b \mid c$ tomando $t = c$. ■

Exemplo 1.7. *Como $MDC(14, 35) = 7$ temos que $MDC(14/7, 35/7) = 1$.*

Teorema 1.9. *Se $a \mid bc$ e $MDC(a,b) = 1$, então $a \mid c$.*

Prova. Como $MDC(a,b) = 1$ pelo Teorema 1.6 existem inteiros n e m tais que $na + mb = 1$. Multiplicando-se os dois lados desta igualdade por c temos: $n(ac) + m(bc) = c$. Como $a \mid ac$ e, por hipótese, $a \mid bc$ então, pela Proposição 1.2, $a \mid c$. ■

Teorema 1.10. *Se a e b são inteiros e $a = qb + r$ onde q e r são inteiros, então $MDC(a, b) = MDC(b, r)$.*

Prova. Da relação $a = qb + r$ podemos concluir que todo divisor de b e r é um divisor de a (proposição 1.2). Esta mesma relação na forma $r = a - qb$, nos diz que todo divisor de a e b é um divisor r.

Logo, o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r, o que nos garante o resultado $MDC(a, b) = MDC(b, r)$. ■

Exemplo 1.8. *Calcule o máximo divisor comum de 1126 e 522.*

$$1126 = 2.522 + 82$$

$$522 = 6.82 + 30$$

$$82 = 2.30 + 22$$

$$30 = 1.22 + 8$$

$$22 = 2.8 + 6$$

$$8 = 1.6 + 2$$

$$6 = 3.2 + 0$$

Para calcular o M.D.C de 1126 e 522, foi utilizado o "Algoritmo da Divisão", (Teorema 1.4). Em seguida dividimos 522 pelo resto 82. Depois pelo resto 30 e assim, sucessivamente, até obtermos resto zero. Portanto, MDC(1126,522)=2.

Exemplo 1.9. *Demonstrar que $MDC(a+b, a-b) \geq MDC(a, b)$. Seja $d = MDC(a,b)$. Então, $d \mid a$ e $d \mid b$*

$$\Rightarrow d \mid (a+b)$$

$$\Rightarrow d \mid (a-b)$$

$$\Rightarrow d \mid MDC(a+b, a-b) \geq d = MDC(a,b).$$

Exemplo 1.10. *Calcule o* $MDC(35n+57, 45n+67)$ *onde n é um inteiro qualquer. Seja* $d = MDC(35n+57, 45n+76)$

$$\begin{cases} d \mid (35n+57) \\ d \mid (45n+76) \end{cases} \Rightarrow \begin{cases} d \mid 9(35n+57) \\ d \mid 7(45n+76) \end{cases}$$

Portanto,

$$d \mid 7(45n+76) - d \mid 9(35n+57)$$

$$d \mid (35n+532-315n-513)$$

$$d \mid 19$$

Logo, $d = 1$ *ou* $d = 19$.

Algoritmo de Euclides

O algoritmo de Euclides serve para determinar o maximo divisor comum de dois números inteiros.

Exemplo 1.11. *Determinar o máximo divisor comum de dois números* 17154 *e* 357, $MDC(17154, 357)$.

Dividendo	*Divisor*	*Resto*	*Quociente*
17154	*357*	*18*	*48*
357	*18*	*15*	*19*
18	*15*	**3**	*1*
15	**3**	*0*	*5*

O máximo divisor comum é o último resto diferente de zero, dividimos o divisor pelo resto da divisão anterior e assim sucessivamente.

Exemplo 1.12. *Vejamos como determinar o máximo divisor comum* (MDC) *entre* 16 *e* 24.

	1	*2* *Quociente*
24	*16*	*8* *M.d.c*
8	*0*	*Resto*

Este processo prático para o cálculo do máximo divisor comum de dois inteiros positivos a e b é denominado algoritmo de Euclides *ou processo das divisões sucessivas.*

É usual o seguinte dispositivo de cálculo no emprego de algoritmo de Euclides*:*

	q_1	q_2	$q_3 \ldots$	q_n	q_{n-1}
a	b	r_1	$r_2 \ldots$	r_{n-1}	r_n
r_1	r_2	r_3	$r_4 \ldots$	0	

Que se traduz na regra: Para "achar" o mdc de dois inteiros positivos, dividi-se o maior pelo menor, este primeiro resto obtido, o segundo resto pelo primeiro, até se encontrar um resto nulo. Então o último resto não nulo é o máximo divisor comum procurado.

1.6 Números Relativamente Primos

Definição 1.11. *Dois números $a, b \in \mathbb{Z}$ são relativamente primos (ou primos entre si), quando $(a,b) = 1$.*

Exemplo 1.13. *Temos que -12 e 35 são primos entre si, pois $mdc(-12, 35) = 1$.*

Teorema 1.12. *Dois números $a, b \in \mathbb{Z}$ ambos não nulos, são relativamente primos, se e somente se, existe x e y tais que $ax + by = 1$.*

Prova. Seja $d = mdc(a, b)$.

($\Rightarrow$) Se $d = 1$, existem x e y inteiros com $ax + by = 1$.

($\Leftarrow$) Reciprocamente, seja $ax + by = 1$ se o $mdc(a, b) = d$, então $d \mid a$ e $d \mid b$. Logo, x e y são inteiros. Daí concluímos que $d \mid 1$. Portanto, $d = 1$, ou seja, a e b são primos entre si. ■

1.7 Mínimo Múltiplo Comum

Definição 1.13. *O mínimo múltiplo comum de dois inteiros positivos a e b é o menor inteiro positivo que é divisivel por a e b.*

Denotado por $[a, b]$ ou $m = mmc(a, b)$, definido pelas duas propriedades:

(i) $a \mid m$ e $b \mid m$ (m é múltiplo comum de a e b)

(ii) Se $a \mid c$ e $b \mid c$ para algum $c \in \mathbb{N}$, então temos também $m \mid c$.

Observe-se que pela condição (i) m é um múltiplo comum de a e b e pela condição (ii), m é o menor dentre todos os múltiplos comum positivos de a e b.

Exemplo 1.14. *$a = 6$ e $b = -8$ os múltiplos comuns dentre a e b são $\{\pm 24, \pm 48, \pm 72, \ldots\}$. Entretanto,*

$$m = mmc(6, -8) = 24.$$

Exemplo 1.15. *Sejam os inteiros $a = -12$ e $b = 30$. Os múltiplos comuns de a e b são $\{\pm 60, \pm 120, \pm 180, \ldots\}$ e como o menor deles é 60. Logo,*

$$m = mmc(-12, 30) = 60.$$

Proposição 1.14. *Se $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_n^{a_n}$ e $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \ldots p_n^{b_n}$, com $a = p_1, p_2, \ldots p_n$ são consideradas os primos que ocorrem nas fatorações de a e b. Vamos denotá-lo por*

$$[a, b] = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \ldots p_n^{\max\{a_n, b_n\}}.$$

Prova. Segundo a definição de mínimo múltiplo comum nenhum fator primo p_i deste mínimo poderá ter expoente que seja inferior nem a a_i e nem b_i.

Suponha, pois, o maior destes dois para expoente de p_i, teremos, não apenas um múltiplo comum, porém o menor possível dentre todos eles. O que conclui o resultado desejado. ■

Proposição 1.15. *Se x e y são números reais então*

$$\max\{x, y\} + \min\{x, y\} = x + y.$$

Prova. Seja $x = y$ então o $\max\{x, y\} = \min\{x, y\} = x = y$ o resultado é trivial. Sem perda de generalidade podemos supor $x < y$.

Portanto, $\max\{x, y\} = y$ e $\min\{x, y\} = x$ e segue-se o resultado desejado. ■

Teorema 1.16. *Quaisquer dois números de Fermat distintos F_n e F_m são relativamente primos.*

Prova. Para provarmos este resultado vamos mostrar, primeiramente, que a seguinte relação se verifica

$$F_0F_1...F_{n-1} = F_{n-2}$$

prova por indução. Como o caso $n = 1$ se verifica, isto é, $F_0 = F_{1-2}$, vamos supor a verificação para n e mostrar que a mesma relação também é verdadeira para $n+1$.

$$\begin{aligned} F_0F_1...F_n &= (F_0F_1...F_{n-1})F_n \\ &= (F_{n-2})F_n \\ &= (2^{2n}+1)(2^{2^n}+1) \\ &= (2^{2n}-1)(2^{2n}+1) = 2^{2n+1}-1 \\ &= 2^{2n+1}+1-2 = F_{n+1}-2. \end{aligned}$$

Agora supondo $n < m$ temos, pela relação acima, que

$$F_0F_1...F_n...F_{m-1} = F_{m-2}$$

o que implica que $F_m - F_0...F_n...F_{m-1} = 2$. Logo, se um número d divide F_n e F_m então d divide 2. Como F_n é impar d não pode ser 2 e portanto, $(F_n, F_m) = 1$ ■

Assim, podemos concluir que existem infinitos números primos, porém sendo infinita a sequência dos números de Fermat e não possuindo fatores comuns, isto não poderia ocorrer se este conjunto fosse finito.

1.8 Equações Diofantinas

Equação diofantina é uma equação em várias incógnitas com coeficientes inteiros. Por exemplo, $3x-2y=1$, $x^3+y^3=z^3$ são equações diofantinas, em homenagem ao matemático grego Diofanto de Alexandria (250 d.C) que escreveu uma importante obra com o título "Aritmética"onde tratou destas e outras equações e suas soluções inteiras.

Diofanto é o primeiro que encontrou soluções das equações justamente chamadas de Diofantinas. Esse tipo de equação, ao ser aplicada pelos matemáticos modernos à análise dos números inteiros, produziram um grande desenvolvimento da teoria dos números. Em particular, Fermat foi levado ao seu "grande" ou "último" teorema quando procurou generalizar um problema que tinha lido na Aritmética de Diofanto: dividir um quadrado dado em dois outros quadrados.

Diofanto, mais que um cultor da Aritmética, e sobre tudo da geométria, como o foram os matemáticos gregos anteriores, deve considerar-se um precursor da álgebra, e, em certo sentido, mais vinculado com a matemática dos povos orientais (Babilônia, Índia,...) que com os gregos. Com a obra de Diofanto houve uma quebra na tradição clássica grega.

A resolução de muitos problemas da Aritmética depende da resolução de Equação do tipo $ax+by=c$, então vamos estudar um pouco o tipo mais simples das equações Diofantinas, isto é, equações do tipo $ax+by=c$.

Uma equação Diofantina é linear se ela tiver a forma:

$$a_1x_1+a_2x_2+a_3x_3+...+a_nx_n=c.$$

Em particular, queremos tratar agora as equações diofantinas lineares do tipo $ax+by=c$ com $a,b,c\in\mathbb{Z}$.

Definição: Uma equação diofantina do primeiro grau a duas variáveis x e y é uma equação do tipo $ax+by=c$ com $a,b,c\in\mathbb{Z}$. Dizemos que a equação tem solução em $\mathbb{Z}$ se existem x_0, $y_0\in\mathbb{Z}$ tais que $ax_0+by_0=c$.

Teorema 1.17. *Sejam $a,b,c\in\mathbb{Z}$, com a,b não nulos.*
a) A equação diofantina

$$ax+by=c \qquad (*)$$

Admite pelo menos uma solução $x,y\in\mathbb{Z}$, se e somente, se $d=MDC(a,b)|c$.
b) Suponha $d|c$ e seja (x_0,y_0) uma solução (particular) de (*). Então a solução de (*) é dada por

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} \quad (t \in \mathbb{Z})$$

Prova. a) Suponha que a equação(*) admite uma solução (x,y), então $ax+by=c$ com $a,b,c \in \mathbb{Z}$. Assim , se $d = MDC(a,b)$, então pelo Teorema 1.6, temos $d|c$.

Reciprocamente, seja $d|c$, digamos $du = c$ para algum $u \in \mathbb{Z}$. Como $d = MDC(a,b)$, então pelo Teorema 1.6, existem $x_1, y_1 \in \mathbb{Z}$ com $d = ax_1 + by_1$. Portanto, $c = a(ux_1) + b(uy_1)$ e assim temos que $(ux_1 + uy_1)$ é uma solução particular de (*).

b) Seja (x_0, y_0) uma solução particular de (*) e $t \in \mathbb{Z}$. Provaremos primeiro que qualquer par de números

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} \quad (t \in \mathbb{Z})$$

satisfaz também a equação:

$$ax + by = a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ba}{d}t = ax_0 + by_0 = c.$$

Seja reciprocamente (x,y) uma solução de (*). Temos $ax_0 + by_0 = c = ax + by$, daí

$$a(x - x_0) = b(y_0 - y).$$

Existem $r,s \in \mathbb{Z}$ tais que $a = rd$ e $b = ds$ segue que $MDC(r,s) = MDC(\frac{a}{d}, \frac{b}{d}) = 1$.

Portanto, $dr(x - x_0) = ds(y_0 - y)$, pois $d \neq 0$. Agora vamos supor $a \neq 0$. Concluímos $r|s(y_0 - y)$ e daí $r|y_0 - y$ então $MDC(r,s) = 1$. Logo, existe $t \in \mathbb{Z}$ tal que $rt = y_0 - y$.

De onde vem $y = y_0 - rt = y_0 - \frac{a}{d}t$. Segue $r(x - x_0) = s(y_0 - y) = srt$ e então $x - x_0 = st$, pois $r \neq 0$, isto nos confirma $x = x_0 + st = x_0 + \frac{b}{d}t$. Logo, temos

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} \quad (t \in \mathbb{Z})$$

para algum $t \in \mathbb{Z}$, como confirmado. ■

Exemplo 1.16. *Ache uma solução inteira da equação:*

$$54x + 21y = 906.$$

Solução: Em primeiro lugar, $mdc(54,21) = 3|906$. Logo, a equação é solúvel e pode ser simplifica para $18x+7y = 302$ com $mdc(18,7) = 1$ e temos que $(2,-5)$ é uma solução de $18x+7y = 1$. Segue que $302 \cdot (2,-5) = (604,-1510)$ isto nos dá como solução

$$\begin{cases} x = 604 + 7t \\ y = -1510 - 187t \end{cases}$$

Exemplo 1.17. *Determine a solução inteira da equação:*

$$143x + 17y = 132.$$

Solução: Temos $mdc(143,17) = 1$, logo a equação tem soluções inteiras. Aplicando o algoritmo de Euclides a 143 e 17. Segue

$$143 = 8 \cdot 17 + 7$$

$$17 = 2 \cdot 7 + 3$$

$$7 = 2 \cdot 3 + 1$$

Logo,
$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot [17 - 2 \cdot 7] = 5 \cdot 7 - 2 \cdot 17 =$
$= 5 \cdot [143 - 8 \cdot 17] - 2 \cdot 17 =$
$= 5 \cdot 143 - 42 \cdot 17$
Donde
$143 \cdot (5 \cdot 132) + 17 \cdot (-42 \cdot 132) = 132$, ou seja, $(x_0, y_0) = (660,-5544)$ é solução da equação.

2 Números Primos

Um número $p \in \mathbb{N}$ é denominado primo, se $p > 1$ e se seus únicos divisores são p e 1. Designaremos por $P = \{p \in \mathbb{N}/p \text{ é } primo\}$, o conjunto de todos os números primos. Se um número inteiro tem módulo maior que um e não é primo, dize-se que é um composto. Por convenção, os números $0, 1$ e -1 não são considerados primos nem composto.

A propriedade de ser primo é chamada "primalidade". Como "dois" é o único número primo par, o termo "primo impar" refere-se a todo primo maior que dois.

Proposição 2.1. *Se $p \mid ab$, p primo, então $p \mid a$ ou $p \mid b$.*

Prova. Se $p \nmid a$, então $(a,b) = 1$ o que implica, pelo Teorema 1.9, $p \mid b$. ■

Assim indicaremos os primos por:

$P = \{2,3,5,7,...1987,...\}$

Os primeiros números compostos são:

$\{4,6,8,9,10,12,14,15,...\}$

Alguns números podem parecer primos como o número $119 = (7 \cdot 17)$ ou $161 = (7 \cdot 23)$. Mas, estes e outros números que têm três ou mais divisores, são considerados compostos.

Teorema 2.2. ***(O Teorema fundamental da aritmétrica)*** *Todo inteiro maior do que* 1 *pode ser representado de maneira única(desconsiderando a ordem) como um produto de números primos (chamados fatores primos) este é o processo de decomposição em fatores primos (fatoração).*

Prova. i) Se n é primo não há nada a ser demonstrado, pois eles podem ser representados de maneira única, como um produto de fatores primos.

Suponhamos, n composto, supondo-se sua unicidade para $p_1 \ \ (p_1 > 1)$ o menor dos divisores de n. Afirmamos que p_1 é primo. Isto nos confirma a verdade, porém, caso contrário, existiria p, $1 < p < p_1$ com $p|n$ então seria contrário a escolha de p_1. Logo, $n = p_1 n_1$.

Novamente seguindo este procedimento, teremos uma sequência decrescente de inteiros positivos $n_1, n_2, ..., n_r$. Como todos eles são inteiros maiores do que 1, então este processo deve terminar.

Como os primos na sequência $p_1, p_2, ..., p_k$ não são, necessariamente distintos, n terá em geral, a forma:

$n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$.

Portanto, n também pode ser escrito como um produto de primos como queríamos provar.

ii) Para a unicidade será feita por indução em n.

Para $n = 2$ a afirmação é verdadeira. Suponhamos maior que 1 e menor que n. Se n é primo não a nada a provar.

Digamos que n seja composto e que tenha duas fatorações, isto é,

$n = p_1 p_2 ... p_s = q_1 q_2 ... q_s$.

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 q_2 ... q^r$ ele divide pelo menos um dos fatores q^j. Sem perda de generalidade podemos supor que $p_1 | q_1$. Como são ambos primos, isto confirma que $p_1 = q_1$.

Logo, $n | p_1 = p_2 ... p_s = q_2 ... q_r$.

Como $1 < n/p_1 < n$, a hipótese de indução nos afirma que as duas fatorações são iguais, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 ... p_s$ e $q_1 q_2 ... q_s$ são idênticas. ■

Teorema 2.3. *Todo inteiro composto possui um divisor primo.*

Prova. Suponha a um inteiro composto. Consideremos o conjunto A de todos os divisores positivos de a, exceto os divisores de 1 e a, isto é,

$$A = \{x | a; 1 < x < a\}$$

Pelo Princípio da Boa Ordenação existe o elemento mínimo p de A. Queremos mostrar que p é primo. De fato, se p fosse composto admitiria pelo menos um divisor d tal que $1 < d < p$, e então $d | p$ e $d | a$, isto é, p não seria o elemento mínimo de A. Portanto, p é primo. ■

Teorema 2.4. *(Euclides) Existe infinitos números primos.*

Prova. Considere um conjunto finito de números primos, contendo uma quantidade arbitrária de elementos. Denotado por $P = \{p_1, ..., p_r\}$. Seja $n = p_1, p_2, ..., p_{r+1}$. com $n \in \mathbb{N}$, então n tem algum fator primo p, ou seja, $p | n$. Então se $p \in P$, seria verdade que $p | 1 = n - (p_1 p_2, ..., p_r)$ devido a linearidade da divisibilidade, pois nem um primo divide 1. Portanto, $p \in P$.

Assim mostrou-se que não importa quantos elementos tenha um certo conjunto de números primos, sempre existirá um outro número primo que não esta em P, o que conclui a prova. ■

Teorema 2.5. *Para qualquer inteiro positivo k existe k inteiros consecutivos todos compostos.*

Prova. Como $(k+1)!$ é divisível por todos os k inteiros consecutivos entre 2 e $k+1$. Então a sequência

$(k+1)!+2, (k+1)!+3, ..., (k+1)!+k, (k+1)!+(k+1)$ é, toda ela composta por k números consecutivos compostos, assim concluímos a demonstração. ■

Exemplo 2.1. *Mostrar que* $(n!+1, (n+1)!+1) = 1$.

Solução: Seja p primo um divisor comum de $n!+1$ e $(n+1)!+1$. Logo, p divide a diferença destes números que é $(n+1)!+1-(n!+1) = n \cdot n!$ o que implica $p|n!$. Como $p|(n!+1), p|(n!+1-n!)$ portanto, $p = 1$ (contradição).

Teorema 2.6. *Se dois inteiros positivos a e b possui as fatorações*

$$a = \prod_{i=1}^{\infty} p_i^{a_i} \qquad e \qquad b = \prod_{i=1}^{\infty} p_i^{b_i}$$

Então o máximo divisor comum de a em b é igual a:

$$(a,b) = \prod_{i=1}^{\infty} p_i^{c_i},$$

onde $c_i = min\{a_i, b_i\}$.

Prova. Para que um produto de fatores primos comuns seja um divisor comum nenhum expoente c_i de p_i poderá superar nem a_i e nem b_i. Como estamos interessados no maior dos divisores positivos, basta tomarmos, para c_i, o menor desses dois. ■

2.1 O Crivo Eratóstenes.

Apresentaremos nesta seção um pouco sobre o célebre ERATÓSTENES, que teve grande importância na Matemática, Astronomia, foi também geógrafo e filósofo grego, nasceu em Cirene por volta de 284 a.C e passou grande parte de sua juventude em Atenas. Com aproximadamente 40 anos, foi convidado pelo rei Ptolomeu III do Egito para ser bibliotecário da Universidade de Alexandria.

Ficou conhecido como Beta, pois por causa de seu saber, foi elevado à condição de um segundo Platão. Outros dizem que tal apelido, lhe fora dado por ter sido o segundo bibliotecário da Universidade de Alexandria. Uma terceira explicação sugere que, apesar de ser talentoso Eratóstenes não conseguiu ser o primeiro de seu tempo em nenhum ramo de estudo, em outras palavras, foi sempre o segundo. Por fim, o históriador James Gow surgeriu que talvez "Beta" indicasse simplesmente o número (Grego) 2 referente a um gabinete ou uma sala de leitura da Universidade.

Escreveu diversas obras, mas, muitas se perderam, inclusive o tratado sobre a medida da terra.

Eratóstenes (no Secúlo III antes de cristo), teve a brilhante idéia de organizar estas maravilhosas computações, na forma bem conhecida de Crivo. Tal crivo serve para determinar todos os números primos, assim como as fatorações dos números compostos, até um dado número

natural.

Teorema 2.7. *Se n não é primo, então n possui, necessariamente, um fator primo menor do que ou igual a* $\sqrt{n}$.

Prova. Seja n composto então $n = n_1 \cdot n_2$ onde $1 < n_1 < n$ e $1 < n_2 < n$. Sem perda de generalidade vamos supor $n_1 \leq n_2$. Logo, n_1 tem que ser $\leq \sqrt{n}$ pois, caso contrário teríamos $n = n_1 n_2 > \sqrt{n}\sqrt{n} = n$ o que é absurdo. Logo, pelo Teorema Fundamental da Aritmética n_1 possui algum fator primo p, este deve ser $\leq \sqrt{n}$. Como p, sendo fator primo de n_1 é também um fator de n, a demonstração está completa. ■

Este resultado nos diz que para testarmos se um número é primo, é suficiente testarmos a divisibilidade apenas pelos primos $\leq \sqrt{n}$. Portanto, se desejarmos obter a lista de todos os primos menores que 60 devemos excluir dentre os números de 2 a 60 aqueles que são múltiplos de $2, 3, 5$ e 7 pois estes são primos $\leq \sqrt{60}$, pois este processo é chamado Crivo de Eratóstenes.

Exemplo 2.2. *Construir a tabela de números primos menores que* 60.

	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
51	52	**53**	54	55	56	57	58	**59**	60

Tabela 1: Os número primos entre 2 e 60

Logo, os primos entre 2 e 60 são todos aqueles que não foram eliminados pelo processo descrito, isto é,

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.$$

2.2 Primos Gêmeos

Definição 2.8. *Chame-se primos Gêmeos dois inteiros positivos ímpares e consecutivos que são ambos primos. Em outras palavras, dizemos que dois primos ímpares são gêmeos quando a diferença entre eles é igual a 2.*

Exemplo 2.3. *São pares de primos gêmeos,* 3 *e* 5*,* 5 *e* 7*,* 11 *e* 13*,* 17 *e* 19*,* 29 *e* 31*,* 41 *e* 43*,* 59 *e* 61*,* 71 *e* 73*,* 101 *e* 103*,* 107 *e* 109*.*

Não sabemos até hoje se há um número infinito de pares de primos gêmeos, porém são conhecidos primos gêmeos muito grandes, tais como:

$$140.737.488.353.507 \quad e \quad 140.737.488.353.509$$

$$140.737.488.353.699 \quad e \quad 140.737.488.353.701$$

Um fato importante e a existência de apenas um terno de inteiros positivos ímpares e consecutivos que são todos primos: $3, 5$ e 7.

Exemplo 2.4. *Mostrar que são primos e que são ímpares consecutivos.*
i) 1949 *e* 1951.

Solução: Primos gêmeos são primos que são impares consecutivos.
Condição(1): 1949 e 1951 são dois impares consecutivos
Condição(2): Devemos verificar se ambos são primos, $452 < 1949$ e $452 < 1951$.

Como ambos não são divisiveis por $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$, os dois são primos.

Logo, os dois primos são gêmeos.
ii) 1997 e 1999.

Solução:
Condição (1): são impares consecutivos.
Condição (2): não são divisiveis por $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$, os dois são primos, logo são primos gêmeos.

2.3 Conjectura de Goldbach

No século XVIII o matemático CHRISTIAN GOLDBACH, numa carta e EULER, conjecturou que todo inteiro par maior que 4 pode ser expresso como soma de dois primos impares. Assim temos:

$$6 = 3 + 3$$

$$8 = 3 + 5$$

$$10 = 3 + 7 = 5 + 5$$

$$12 = 5 + 7$$

$$14 = 3 + 11 = 7 + 7$$

$$16 = 3 + 13 = 5 + 11$$

$$18 = 5 + 13 = 7 + 11$$

.....

Muitos matemáticos têm procurado demonstrar a conjectura de GOLDBACH, mas nada foi conseguido até hoje.

2.4 Tipos Especiais de Números Primos

2.4.1 Números Primos Fatoriais

Um número primo p é chamado de fatorial se ele está na forma:

$$p = n! \pm 1$$

Para algum número n, onde n pode ser representado pela forma:
$n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot n = \prod_{k=1}^{n} k$, para todo inteiro $n \geq 0$. Os primeiros primos fatoriais são:

n	1	2	3	3	4	6	7	11	12	14
p	2	3	5	7	23	719	5039	39911681	479001599	87178291199

Tabela 2: Números Primos Fatoriais

2.4.2 Números Primos de Mersenne

Um número da forma $M(n) = 2^n - 1$, com $n = 2,3,4,7,...$ é chamado de MERSENNE. Assim, a sequência dos números de MERSENNE são

$$M_{n\geq 2} = (3,7,15,31,63,127,255,511,1023,...,2^n - 1,...)$$

Um número $M(n)$ se diz número primo de Mersenne se puder ser escrito na forma:

$$M(n) = 2^n - 1$$

com n natural.

Em agosto de 2007, apenas 44 primos de Mersenne eram conhecidos. O maior número primo conhecido atualmente é um número de Mersenne $(2^{32.582.667} - 1)$. Os primos de Mersenne foram observados primeiramente por Euclides, mas apenas no século $XVII$, o estudante francês Marin Mersenne compilou uma lista dos primos de Mersenne com expoentes até 257.

Exemplo 2.5. *Os primeiros primos de MERSENNE para* $p = 2,3,5,...$

$$M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127, M_{13} = 8191, M_{17} = 131071, M_{19} = 524287, M_{31}...$$

Portanto, os primeiros primos de Mersenne são:

n	$M_{(n)}$
2	3
3	7
5	31
7	127
13	8191
17	131071
19	524287
31	2147483647
61	2305843009213693951

Tabela 3: Números Primos de Mersenne

2.4.3 Números Primos Titânicos

Foi na década de 80 que Samuel Yates iniciou uma lista dos "Maiores Primos conhecidos" e chamou de primos titânicos. Hoje em dia, são conhecidos uma infinidade de primos titânicos. Os primeiros números primos Titânicos são de várias formas, sendo os maiores os números de Mersenne primos e os restantes da forma:

$$k \cdot 2^n \pm 1$$

$$k^2 \cdot 2^n + 1$$

$$k^4 \cdot 2^n + 1$$

$$k \cdot 10^n + 1$$

$$\left(\frac{10^n - 1}{9}\right)$$

Esta expressão é utilizada para denominar todos os números primos que possuam mais do que 1.000 digítos.

2.4.4 Números Primos de Fermat

Um número primo de Fermat é um inteiro positivo que assume a forma $F = 2^{2^n} + 1$, sendo n um inteiro não negativo. Os primeiros números de Fermat são:

$$F^0 = 3, F^1 = 5, F^2 = 7, F^3 = 257, F^4 = 65537.$$

Pierre de Fermat conjecturou que todo número de Fermat é primo de fato, os primeiros cinco números de F_0 e F_4 são primos. Porém, esta conjectura foi contestada por Leonhard Euler em

1732 quando ele mostrou que F_5 era um número composto. Os únicos números primos de Fermat conhecidos são os números de F_0 até F_4.

Portanto, poucos primos de Fermat são conhecidos. Muitos dos maiores números primos conhecidos são generalizados dos primos de Fermat. Até hoje não se descobriu nenhum número $F(n)$ primo com $n \geq 5$.

2.4.5 Números Primos de Wilson

Em homenagem ao matemático John Wilson, designa-se que dado "p" número primo, então $(p-1)! \equiv (mod\ \ p)$. Logo, o quociente de Wilson:

$$W(p) = \frac{(p-1)!+1}{p}$$

é um inteiro.

O número p é chamado primo de Wilson quando $W(p) \equiv 0(mod\ \ p)$, ou seja, um número primo p é um primo de Wilson se p^2 divide $(p-1)!+1$, onde "!" denota a função fatorial. São exemplos de primos de Wilson os números 5 e 13. Além de 5 e 13, foi descoberto por Goldberg em 1953 que o número 563 é um número primo de Wilson.

2.4.6 Números Primos de Wall-Sun-Sun

Um primo de Wall-Sun-Sun é um certo tipo de número primo que é conjecturado existir embora nenhum seja conhecido. Também um número primo $p > 5$ é considerado de primo de $Wall - Sun - Sun$ se p^2 divide $F(P - (\frac{P}{5}))$, onde $F(n)$ é o enésimo número de Fibonacci.

2.4.7 Números Primos de Smarandache-Wellin

É definido como um número inteiro formado pela concatenação dos n primeiros números primos. Os primeiros números de Smarandache-Wellin são:

$$2, 23, 235, 2357, 235711, ...$$

Um número de Smarandache-Wellin que é primo, ele é chamado de primo de Smarandache-Wellin. Os índices dos primeiros primos de Smarandache-Wellin na base decimal são:

$$1, 2, 4, 128, 174, 342, 435.$$

2.4.8 Números Primos de Wieferich

Primos de Wieferich, são números primos p onde p^2 divide $2^{p-1} - 1$. Foram escritos por Wieferich em 1904 e existe apenas dois conhecidos 1093 e 3511.

2.4.9 Números Primos de Truncáveis

Um primo Truncáveis, é um número que não contém nenhum zero e se um digíto de uma das pontas for retirado sucessivamente o número resultante também deve ser primo, por exemplo, 1223 é um primo Truncáveis à esquerda, pois, 223, 23 e 3 são todos primos. Existem 4260 primos Truncáveis a esquerda na base decimal. os primeiros são:

$$(2,3,5,7,13,17,23,37,43,53,67,73,83,97,113,137,167,173,etc.)$$

O maior primo Truncável a esquerda tem 24 dígitos:

$$357686312646216567629137.$$

Existem 83 primos Truncáveis a direita. Os primeiros são:

$$2,3,5,7,23,29,31,37,53,59,71,73,79,233,239,293,311,313,317,etc.$$

O maior primo Truncável a direita tem 8 dígitos:

$$73939133.$$

Existem também os primos Truncáveis de dois lados, no qual um dígito pode ser retirado tanto da esquerda quanto da direita, pois, o resultado continua sendo primo. Os números são:

$$2,3,5,7,23,37,53,73,313,317,373,797,3137,3797,739397.$$

2.4.10 Números Primos de Sophie Germain

Se p é um número primo de Sophie Germain, então não existem números inteiros, x,y,z diferentes de zero e não múltiplos de p, tais que $x^p + y^p = z^p$. É também primo p de Sophie Germain se $2p+1$ é primo. São famosos porque Sophie Germain provou que o último teorema de Fermat é verdadeiro para estes números. A existência de um número inteiro de tais números primos é um conjectura, ou seja, uma afirmação não provada. Há 190 números primos de Sophie Germain no intervalo $[1,10^4]$. Os primeiros primos de Sophie Germain são:

$$2,3,5,11,23,29,41,53,83,89,113,131,173,179,191,233...$$

O maior número primo de Sophie Germain conhecido até hoje é o número $2^{265440}-1$ que tem 79911 dígitos e foi descoberto em março de 2010.

2.4.11 Números Primos de Fibonacci

Os números de Fibonacci recebe o nome de sequência de Fibonacci que obdecem a seguinte função recorrente.

$$F(n) = \begin{cases} 0, se \;\; n = 0; \\ 1, se \;\; n = 1; \\ F(n-1) + F(n-2), \quad se \;\; n > 1. \end{cases}$$

Assim, depois dos dois primeiros valores, cada número é a soma dos dois números anteriores. É óbvio que se pode construir arbitrariamente uma sequência infinita de números de inteiros. Primeiros números de Fibonacci são

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F_n	0	1	1	2	3	5	8	13	27	34	55	89	144	233	377	610

Tabela 4: Números de Fibonacci

Um número primo de Fibonacci é um número primo que faz parte da sequência de Fibonacci. Os primeiros dez números primos de Fibanacci são:

$$2, 3, 5, 13, 89, 233, 1597, 28657, 514229, 433494437.$$

s

Conclusão

Ao longo do nosso trabalho fizemos um relato histórico sobre a Teoria dos Números e dos Números Primos e vimos o seu desenvolvimento durante os séculos. Nos dias atuais, as aplicações dessa teoria é necessária para o desenvolvimento tecnológico das senhas de contas de bancos, email etc. Finalmente, estudamos os principais tipos especiais de números primos, e observamos a existência de vários pesquisadores em Teoria dos Números, na qual a todo momento surgem novos tipos de primos.

Referências

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*, IMPA 2003.

DOMINGUES, Higyno; IEZZE, Gelson.*Álgebra moderna, atual, 4ed.*.São Paulo: Atual, 2003.

EVES, Howard, *Introdução à Historia da Matemática*.Campinas-SP: Editora da UNICAMP, 2004.

FILHO, Edgard de Alencar.*Teoria Elementar dos Números*, 2º ed. São Paulo: Nobel, 1985.

GODINHO, H.T; SOARES,M.; SHOKRANIAN,S.,*Teoria dos Números*, UNB, 2004.

MAIER, Rudolf,*Teoria dos Números (NOTAS DE AULAS)*, 2005.

SANTOS, José Plínio de OLiveira.*Introdução à Teoria dos Números*.Rio de Janeiro: IMPA 2006.