m

Universidade Federaql da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado Profissional em Matemática

Números Primos [†]

por

José Cleiton Rodrigues Padilha

Prof. Bruno Henrique Carvalho Ribeiro

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Setembro/2013
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Números Primos

por

José Cleiton Rodrigues Padilha

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

área de Concentração: Matemática-Teoria dos Numeros-Números Primos.

Aprovada por:

Prof. Dr. Bruno Henrique Carvalho Ribeiro -UFPB (Orientador)

Prof. Dr. Cleto Brasileiro Miranda Neto - UFPB

Prof. Henrique de Barros Correia Vitorio - UFPE

Setembro/2013

Agradecimentos

Quero agradecer a todos aqueles que de forma direta ou indiretamente, contribuíram para mais este passo dado. Em particular a CAPES e a UFPB, pelos apoios financeiro e acadêmico. Ao professor Dr. Bruno Henrique Carvalho Ribeiro, pela sua valorosa orientação, em especial a Ana Cláudia Padilha e aos três grandes companheiros aos quais tive em minha jornada: Gleidson, Duda Jorge e Luiz.

O Autor

Dedicatória

A todos os que se alegram com o nosso sucesso.

Resumo

O propósito deste trabalho é apresentar uma categoria especial de números inteiros: Os Números Primos.

Será apresentada uma retrospectiva histórica, citando os resultados mais importantes e interessantes obtidos por grandes matemáticos ao longo dos anos. Em seguida, a maioria destes resultados serão formalmente enunciados com proposições ou teoremas e suas respectivas demonstrações, começando com as propriedades básicas da divisibilidade e culminando em alguns testes de primalidade.

Palavras-chave: Teoria dos Números. Números Primos. Distribuição dos números primos. Teste de primalidade.

Abstract

The purpose of this work is to present a special category of integers: Prime numbers.

It will be presented a historical retrospective, quoting the most important and interesting results achieved by great mathematicians over the years. Then, most of these results will be formally announced with propositions or theorems and their respective demonstrations, starting with the basic properties of divisibility and culminating in some primality tests.

Keywords: Number Theory, Prime Numbers. Prime Numbers distribution. Primality test.

Sumário

Introdução

Desde da Grécia Antiga os matemáticos se interessam pelos números primos: Quantos são? Como se distribuem? Como encontrá-los? Existe uma maneira simples de saber se um número é primo ou não?

No decorrer dos séculos algumas destas perguntas foram respondidas, outras ainda permanecem sem resposta até os dias atuais. Por exemplo, até hoje não se sabe precisamente como os números primos se distribuem entre os números compostos (os que não são primos), nem como descobrir, de maneira simples, se um número é primo ou não.

Os gregos foram os primeiros a perceberem que os números primos eram os "átomos", os blocos básicos, com os quais se poderiam construir todos os números naturais pela multiplicação, exceto o 1.

Os pitagóricos, em sua veneração pelos números, também já os conheciam.

Contudo, foi somente nos Livros VII, VIII e IX, da obra Os Elementos, de Euclides, dedicados 'a Teoria dos Números, que os primos revelaram-se formalmente. Conforme consta em [12], p. 79:

> *"O Livro IX, o último dos três sobre Teoria dos Números, contém vários teoremas interessantes. Desses, o mais célebre é a Proposição 20: 'Números primos são mais do que qualquer quantidade fixada de números primos.' Isto é, Euclides dá aqui a prova elementar bem conhecida do fato de que há infinitos números primos. A prova é indireta, pois mostra-se que a hipótese de haver somente um número finito de primos leva a uma contradição."*

Outra questão curiosa é sobre com que frequência um número primo aparece. Quando se observa uma lista de primos se nota, num breve olhar, que existem diversos pares de números primos que diferem apenas por duas unidades, tais como 3 e 5, 5 e 7, 11 e 13, 17 e 19, entre outros. Mas como estão distribuídos os números primos? Há grandes sequências de números naturais em que os primos não aparecem? E como saber se um número é primo? Com a intenção de responder algumas dessas perguntas, essa pesquisa foi organizada em quatro capítulos.

No capítulo 1, apresentamos uma retrospectiva sobre a vida de alguns matemáticos, focando suas descobertas sobre os números primos, partindo dos antigos gregos do século I a.C., passando pelos séculos XVII e XVII, com nomes como Euler e Gauss, e chegando até Riemann.

No capitulo 2, tratamos de conceitos básicos relacionados a divisibilidade, demostrando o Algoritmo de Euclides e o importante Teorema Fundamental da Aritmética. Neste capítulo introduzimos as noções de congruências e mostramos dois resultados essenciais da teoria dos números, são eles: a existência de infinitos números primos e lindo postulado de Bertrand.

Adiante, no capítulo 3, exibimos três resultados relacionados a decidir se um dado número será primo ou não. Focamo-nos no Crivo de Eratóstenes, no Pequeno Teorema de Fermat e sua generalização, com o teorema de Euler, e no Teorema de Wilson.

No último capítulo, aparecem alguns resultados sobre os números de Mersenne e os números de Fermat, embora este já tenha sido tratado no capítulo 1. Trazemos ainda um tópico sobre os primos em uma progressão aritmética e a demonstração do belíssimo produto de Euler.

Ao final, no apêndice A, relatamos resultados que usamos nos capítulos anteriores, porém sem nos preocuparmos com formalismo

Capítulo 1

Uma Retrospectiva no Estudo dos Números Primos

Neste capítulo apresentaremos uma breve retrospectiva a respeito de algumas descobertas, de eminentes matemáticos, ligadas a Teoria dos Números.

Tais descobertas contribuíram, enormemente, para o desenvolvimento deste ramo da matemática, e, em particular, para o conhecimento das propriedades relativas aos números primos.

1.1 Números Primos

Número é um conceito fundamental em Matemática que tomou forma num longo desenvolvimento histórico. A origem e formulação deste conceito ocorreram simultaneamente com nascimento e desenvolvimento da Matemática. As exigências da própria matemática e a necessidade do homem alavancaram o desenvolvimento deste importante conceito.

A Teoria dos Números trata principalmente das propriedades dos números inteiros positivos $1, 2, 3, 4, 5, ...$ A noção de inteiro positivo é talvez a mais importantes e mais clara de todos os conceitos matemáticos. Apesar disto, é fácil formular questões elementares envolvendo estes números, que não podem ser respondidas, mesmo com os recursos mais profundos da matemática moderna.

É óbvio que todo inteiro positivo é divisível por 1 e por si mesmo. Se um inteiro $p > 1$ não tem divisores positivos, exceto 1 e p este chama-se *número primo* ou simplesmente *primo*; caso contrário, diz-se *composto*. Apesar de simples e de sua definição ser de fácil compreensão, jamais poderíamos imaginar a complexidade que este conceito envolve.

Os números primos e suas propriedades foram estudados exaustivamente pelos matemáticos da antiga Grécia, que dividiam os números em *primeiros* ou *indecomponíveis* e *secundários* ou *compostos*. Os compostos são secundários, pois são formados

a partir dos primeiros. Os romanos traduziram a palavra grega para primeiro, que em latim é *primus*.

O estudo destes elementos são realizados desde, aproximadamente, 500 a.C. Os pitagóricos (500 - 300 a.C.) interessavam-se em compreender a razão de ser dos números inteiros, procurando explicar através deles a essência de todas as coisas.

Atualmente um aspecto importante é que os números primos são extremamente importantes na Criptografia[1].

Nas próximas seções, descreveremos um breve histórico da vida de matemáticos da antiguidade, que pelos nossos conhecimentos, mais contribuíram para o desenvolvimento da teoria sobre os números primos.

1.2 Pitágoras

Pitágoras de Samos é um dos personagens mais conhecidos e talvez o mais misterioso na história da matemática. Nasceu em Samos, na costa oeste da Ásia Menor, morreu em Metapontum em idade avançada.

Pitágoras viajou cerca de 30 anos pelo Egito, Babilônia, Fenícia, Síria e possivelmente indo até a Índia e Pérsia. Durante suas jornadas ele absorveu a cultura local, assimilando o conhecimento matemático e astronômico desses povos. Estabeleceu-se em Crotona. Fundou uma escola que ficou conhecida como "Escola Pitagórica", onde um dos interesses era pelos números e misticismo ligado a eles.

Os pitagóricos, assim chamados os que frequentavam esta irmandade, distinguiram conceitos entre números primos, compostos e número perfeito[2]. Não se pode desconsiderar a influência dos Pitagóricos nos Elementos de Euclides.

1.3 Euclides

O nome de Euclides está ligado a geometria em sua famosa obra *"Os Elementos"*[3], quando este apareceu muitos dos resultados importantes sobre números pri-

[1] É o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário. De fato, o estudo da criptografia cobre bem mais do que apenas cifrar e decifrar códigos. É também um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática como a teoria dos números.

[2] Número Perfeito é um número inteiro positivo para o qual a soma de todos os seus divisores positivos próprios (excluindo ele mesmo) é igual ao próprio número. Por exemplo, o número 6 é um número perfeito, pois:$1 + 2 + 3 = 6$

[3] Os Elementos constituem um tratado matemático e geométrico composto por 13 livros escrito por volta de 300 a.C.. Ele engloba uma coleção de definições, postulados, proposições, teoremas, construções e provas matemáticas das proposições. Os treze livros cobrem a geometria euclidiana e a versão grega antiga da Teoria dos Números Elementar.

Figura 1.1: Pitágoras Samos

mos já tinham sido provados.

Quando percorremos a sequência dos números inteiros positivos, observamos que os primos parecem ocorrer cada vez com menos frequência. Tal observação é bem razoável; é mais plausível que seja composto um "número grande" que um "número pequeno", pois ele está além de uma quantidade maior de números que podem ser seus fatores. É ainda concebível que os primos existam em uma quantidade finita e que todos os outros números sejam compostos.

A demonstração de que essa ideia não é verdadeira, ou seja, de que há uma infinidade de números primos, é uma das primeiras demonstrações feitas por redução ao absurdo. Feita por Euclides, a demonstração é muito simples: para tanto suponhamos que há uma quantidade finita de números primos $p_1, p_2, p_3, ..., p_n$, consideremos agora o número $N = p_1p_2p_3...p_n + 1$ que não é divisível por nenhum dos p_i, com $1 \leq i \leq n$. Portanto N é primo, o que contradiz a suposição de que existe uma quantidade finita de números primos. Este resultado aparece na Proposição 20 do Livro IX dos Elementos. Ainda neste livro aparece o teorema de Euclides sobre os números perfeitos, onde nos diz que sendo n um inteiro positivo, para o qual $2^n - 1$ é primo, então $2^{n-1}(2^n - 1)$ é um número par perfeito.

Alguns outros itens de interesse especial são: No Livro VII o Algoritmo Euclidiano, um processo para se achar o máximo divisor comum de dois inteiros positivos, o Lema de Euclides, que nos diz se um número primo divide o produto de dois números inteiros positivos então ele necessariamente divide um deles.

Figura 1.2: Euclides de Alexandria

1.4 Eratóstenes

Eratóstenes nasceu em Cirene, uma colônia grega do Norte da África, por volta do ano 276 a.C. e morreu em Alexandria por volta de 196 a.C.. Foi um matemático e um grande estudioso em outras várias áreas, além de ter sido bibliotecário da grande biblioteca e Alexandria. Em matemática Eratóstenes trabalhou também com aritmética, e é lembrado, principalmente, pela importantíssima ferramenta para determinar números primos, chamada *Crivo de Eratóstenes*.

Alguns séculos depois, durante a Idade Média, o desenvolvimento da teoria dos números ficou estagnado, assim como praticamente todas as outras áreas do conhecimento. Somente no século XVII, após estudar a Arithmetica de Diofanto (escrita provavelmente no século III), Pierre de Fermat ressuscitou a questão, e é considerado o fundador da moderna Teoria dos Números.

1.5 Fermat

Pierre de Fermat, 17 de agosto de 1601 Beaumont-de-Lomages, 12 de janeiro de 1665, Castres, França.

Foi talvez o maior matemático do século XVII, mas sua influência foi limitada por falta de interesse em publicar suas descobertas. Era advogado e membro da Suprema Corte de Toulouse, França. Entretanto seu passatempo e sua paixão particular era a matemática.

Fermat se correspondia com outros matemáticos de sua época, em particular com o monge Marim Mersenne.

Em uma de suas cartas a Mersenne, ele conjecturou que os números $2^n + 1$ eram

sempre primos se n é uma potência de 2. Ele havia verificado isto para os casos em que n era igual a $1, 2, 4, 8$ e 16 e sabia que se n não era uma potência de 2, o resultado falhava.

Os números desta forma são chamados *Números de Fermat*, um século depois, Euler demonstrou que $2^{32}+1$ é divisível por 641 e portanto não é primo. Os números da forma $2^n - 1$ atraíram também a atenção de Fermat, pois era mais fácil mostrar que a menos que n seja primo este número será composto. Adiante falaremos destes resultados.

Sobre o trabalho de Fermat nesse campo, não se pode deixar de falar do resultado que se segue, conhecido como *O Pequeno Teorema de Fermat*, onde diz que se p é um primo e n um inteiro positivo, não divisível por p, então p divide $n^{p-1} - 1$.

Este teorema é de fundamental importância em teoria dos números, assim como em outros ramos da matemática como em álgebra moderna, por exemplo.

Falando de Fermat, não podemos deixar de mencionar sua mais famosa proposição, conhecida como *Ultimo Teorema de Fermat*, onde ele afirma, mas não demonstra, que a equação $x^n + y^n = z^n$, sendo x, y, z e n são inteiros e $n \geq 3$ não possui soluções inteiras não nulas, só demonstrada cerca de 300 anos depois pelo matemático inglês Andrew Wiles em 1996.

A teoria dos números dos século XIX foi fortemente impulsionada pelos grandes resultados de Fermat nessa área.

Figura 1.3: Pierre de Fermat

1.6 Mersenne

Marin Mersenne era um monge franciscano que vivia num mosteiro em Paris, nasceu em Oizé em 8 de Setembro de 1588 e morreu em 1 de Setembro de 1648, em

Paris.

Apesar de seus estudos em várias áreas da ciência,para a matemática sua contribuição foi em teoria dos números, estudando os números da forma $2^n - 1$. Mersenne conhecia a prova de Euclides sobre os números perfeitos, ele também sabia que $2^n - 1$ não era primo se n não fosse. Assim foi levado ao problema de determinar para quais números primos p, $2^p - 1$ seria primo, pois para alguns valores de p este será um número composto.

Em 1644 Mersenne afirmou que entre os primos menores que 258 os únicos para os quais $2^p - 1$ são também primos, são:$2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, mas não deu nenhuma evidência que o levasse a tal afirmação, hoje sabe-se que ele cometeu dois erros: 67 e 257 não pertencem a lista. Em 1903, o matemático americano F. N. Cole anunciou a fatorabilidade de $2^{67} - 1$ e em 1913, D. H. Lehmer provou que $2^{257} - 1$ é também composto.

1.7 Euler

Leonhard Paul Euler nasceu na Basileia Suiça em 15 de abril de 1707 e morreu em São Petersburgo, Rússia em 18 de setembro de 1783.

Euler foi talvez o autor mais prolixo de todos os tempos, acrescentando conhecimentos a todos os ramos conhecidos da matemática pura e aplicada. Dentre suas varias contribuições ele foi o primeiro grande mestre no estudo das séries e produtos infinitos. Em 1736, estudando a função, definida como

$$f(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Euler fez a maravilhosa descoberta $f(2) = \dfrac{\pi^2}{6}$ ou seja

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + ... = \frac{\pi^2}{6}$$

.

Em teoria dos números, Euler buscou muitas de suas inspirações nas desafiantes notas deixadas por Fermat. Foi o primeiro a publicar a prova do Pequeno Teorema de Fermat e também demonstrou uma outra famosa afirmação de Fermat, onde ele diz que "um primo da forma $4n + 1$ se pode expressar como a soma de dois quadrados perfeitos de forma única, também que um número da forma $4n - 1$ não pode ser decomposto de nenhuma forma como soma de quadrados perfeitos". De suas correspondências com Cristian Goldbach surgiu a hoje conhecida como *Conjectura de Goldbach*, onde afirma que todo número par maior do que 4 é soma de dois primos.

Euler foi o primeiro a notar que a teoria dos números pode ser estudada através das ferramentas da análise matemática. Uma grande resultado derivado dessa visão de Euler é a famosa identidade, importantíssima no estudo da distribuição dos primos em que, sendo $s > 1$

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\ primo} \frac{1}{1 - \frac{1}{p^s}} \tag{1.1}$$

Euler também demonstrou que existiam infinitos primos da forma $4n + 1$, e chegou a conjecturar a existência de infintos primos em qualquer progressão aritmética $a, a + b, a + 2b, a + 3b, ..., a + nb$ sendo a e b primos entre si, conjectura esta que foi provada, em 1837 por Dirichlet.

Figura 1.4: Leonhard Euler

1.8 Gauss

Johann Carl Friedrich Gauss, nasceu em Brunswick, norte da Alemanha, em 30 de Abril de 1777 e morreu em 23 de Fevereiro de 1855 na cidade de Göttingen, Alemanha.

Sua extraordinária habilidade com os números ficou evidente desde muito cedo. Ele iniciou suas breves notas no seu diário científico num esforço de guardar suas descobertas, uma vez que havia muitas para serem trabalhadas naquela época. A primeira nota feita por Gauss explica a construtibilidade do polígono regular de 17 lados, porém antes disso ele já havia penetrado em campos inexplorados da teoria dos números.

Em 1795 ele descobriu a Lei da Reciprocidade Quadrática, onde afirma que se p e q são dois números primos ímpares distintos então

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

.

Onde $\left(\frac{p}{q}\right)$ é o *símbolo de Legendre.*

Gauss não sabia que o teorema havia sido mal formulado e deixado sem demonstração por Euler e corretamente formulado e incorretamente demonstrado por Legendre. Este é o cerne da parte central do seu famoso tratado *Disquisitiones Aritmeticae*, publicado em 1801, que é usualmente considerado como um marco do início da moderna teoria dos números.

Nas páginas introdutórias de seu *Disquisitiones Aritmeticae*, Gauss desenvolve seu método de congruências para o estudo de problemas de divisibilidade e dá a primeira demonstração do Teorema Fundamental da Aritmética, que afirma que todo números inteiro $n > 1$ pode ser esdrito de forma única com produto de primos. A parte central é dedicada principalmente às congruências quadráticas, formas e resíduos. A ultima seção apresenta sua teoria do polinômio ciclotômico com suas aplicações à contrutibilidade de polígonos regulares.

Outro grande trabalho na área da teoria dos números foi um artigo de 1831 sobre resíduos biquadráticos, onde ele estendeu algumas de suas descobertas anteriores, por um caminho puramente algébrico, para estudar os números complexos, onde seu objetivo era divulgar as ideias de teoria dos números para o domínio dos números complexos, definindo os inteiros complexos, hoje chamados de inteiros gaussianos, como sendo números complexos $a+bi$ com a e b inteiros, introduziu um novo conceito de número primo no qual 3 permanece primo, mas $5 = (1+2i)(1-2i)$ não, e provou o teorema da fatorização única para esses inteiros e primos.

As ideias desse artigo inauguraram a Teoria Algébrica dos Números[4].Assim, Gauss contribuiu largamente para a estruturação da teoria dos números.

1.9 Dirichlet

Johann Peter Gustav Lejeune Dirichlet, Düren, 13 de fevereiro de 1805 e morreu Göttingen, 5 de maio de 1859. foi um matemático alemão que fez muitas contribuições de grande valor para a análise e para a Teoria dos Números. Foi profundamente influenciado por seu encontro e contato por toda sua vida com Disquisitiones Arithmeticae, de Gauss.

[4]Teoria algébrica dos números é um ramo da teoria dos números em que o conceito de número é expandido para o de número algébrico, que são raízes de polinômios com coeficientes racionais.

Figura 1.5: Gauss

O trabalho de Gauss continha muitas descobertas de longo alcance dos grandes mestres em Teoria dos Números, mas era compreendido por muitos poucos matemáticas naquele tempo. Dirichlet foi o primeiro que não somente entendeu-o completamente mas também tornou-o acessível aos outros.

Mas tarde Dirichlet ficou amigo e discípulo de Gauss, e também um amigo e orientador de de Riemann, a quem ele ajudou um pouco em sua tese de doutoramento.

Em 1855, depois de lecionar em Berlim por muitos anos, ele sucedeu Gauss em Göttigen.

Talvez seus maiores trabalhos tenham sido as duas longas memórias de 1839 nas quais ele fez aplicações da análise à Teoria dos Números. Foi na primeira delas que ele provou seu belo teorema de que existem infinitos números primos em qualquer progressão da forma $a + nq$ com a e q primos entre si. Suas descobertas sobre séries absolutamente convergentes também apareceram em 1837.

1.10 Riemann

Georg Friedrich Bernhard Riemann nasceu em Breselenz, Reino de Hanôver em 17 de Setembro de 1826 e faleceu em Selasca, Verbania, 20 de Julho de 1866. Foi um matemático alemão, com contribuições fundamentais para a análise e a geometria diferencial. Ele estudos os trabalhos de Euler e de Legendre quando ainda estava no curso secundário, e diz-se que dominou o tratado de Legendre sobre a teoria dos números em menos de uma semana.

Em 1859, Riemann publicou seu único trabalho em teoria dos números, um breve mas extremamente profundo artigo de menos de dez páginas, dedicado ao Teorema

dos Números Primos[5]. Esse esforço poderoso iniciou grandes ondas em vários ramos da matemática pura. Seu ponto de partida foi uma identidade notável[6], descoberta por Euler no século anterior.

O próprio Euler explorou essa conexão de vários modos, mas Riemann percebeu que o acesso aos resultados mais profundos da distribuição dos primos pode ser obtido apenas permitindo que a variável s seja complexa.

Riemann denotou a função por $\zeta(s)$, e ficou conhecida desde então como a função zeta de Riemann:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots \text{, onde } s = a + bi$$

Em seu artigo, ele provou várias propriedades importantes dessa função, e enunciou uma quantidade de outras sem prová-las. Durante um século a partir de sua morte, muitos dos matemáticos mais brilhantes do mundo exerceram seus maiores esforços e criaram novos ricos ramos da Análise na tentativa de provar esses enunciados. O primeiro sucesso foi alcançado por J. Hadamard, em 1893, e com uma única exceção todos os resultados foram confirmados no sentido que Riemann esperava[7].

Essa exceção é a famosa hipótese de Riemann: que afirma que todos os zeros de $\zeta(s)$ na faixa $0 \leq a \leq 1$ caem na linha central $a = 1/2$. Ela permanece hoje como o problema em aberto mais importante da matemática.

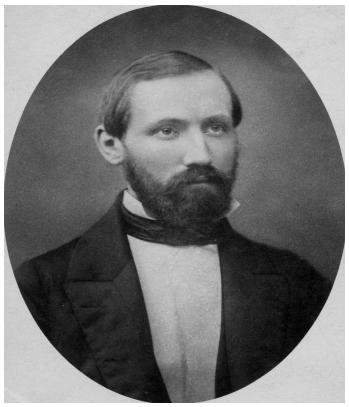

Figura 1.6: Riemann

[5]O Teorema do Número Primo é um importante resultado sobre a distribuição dos números primos, onde afirma que sendo $\pi(n)$ o número de primos entre 1 e n, inclusive, então

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1$$

[6]Veja equação 1.1.

[7]O trabalho de Hadamard levou-o a sua prova do Teorema dos Números Primos, em 1896.

Capítulo 2

Números Primos

Neste capítulo descreveremos as algumas propriedades relativas à divisão entre números inteiros e o Algoritmo de Euclides, a noção de congruências e algumas de suas propriedades, a distribuição dos números primos e o postulado de Bertrand.

2.1 Divisibilidade

Abordaremos nesta seção o Algoritmo de Euclides que é a principal ferramenta para se estudar a divisão entre números inteiros.

Definição 2.1.1. Sejam a, b números inteiros, dizemos que a divide b e escrevemos $a|b$ se existir x, também inteiro, tal que: $b = ax$. Nestas condições dizemos também que a é um divisor de b, ou que b é um múltiplo de a. Escreveremos $a \nmid b$ se a não dividir b.

Propriedades da divisibilidade

Sejam a, b e k números inteiros, com a e b não nulos. Temos que:

1. $1|k$, $k|k$ e $a|0$.
2. Se $a|b$ e $b|k$ então $a|k$.
3. Se $a|k$ e $a|b$ então $a|(b+k)$
4. Se $a|k$ então $a|bk$.

Demonstração:

1. Estes fatos decorrem das respectivas igualdades: $k = k.1$, $k = 1.k$ e $0 = a.0$.

2. Se $a|b$ e $b|k$, então existem inteiros x e y tais que: $b = x.a$ e $k = b.y$.Assim:

$$k = (x.a).y = (x.y).a \Rightarrow a|k.$$

3. Se $a|k$ e $a|b$ existem x e y inteiros tais que $k = xa$ e $b = ay$. Portanto:

$$b + k = (x + y)a \Rightarrow a|(b + k).$$

4. Se $a|k \Rightarrow k = x.a$, com x inteiro, então:

$$b.k = (b.x).a \Rightarrow a|bk \quad \blacksquare$$

Proposição 2.1.1. Sejam n, a, b inteiros, com $n \geq 0$ e $a \neq b$. Temos que

$$(a - b)|(a^n - b^n).$$

Demonstração:

Seja $P(n)$ a afirmação a ser provada, usaremos indução sobre n para verificar sua validade.

Vemos que $P(0)$ é verdade, pois se $n = 0$ $a^n - b^n = a^0 - b^0 = 0$ e $(a - b)|0$.

Suponhamos $P(n)$ verdadeira e vamos considerar a expressão $a^{n+1} - b^{n+1}$. Então:

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

Pela hipótese indutiva $(a - b)|(a^n - b^n) = k(a - b)$, com k inteiro. Assim:

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

Logo $(a - b)|a^{n+1} - b^{n+1}$. $\blacksquare$

2.2 O Algoritmo de Euclides

Provaremos agora o Algoritmo de Euclides que é uma poderosa ferramenta da aritmética, que embora com mais de 2 mil anos, pois apresentado nos *Elementos*, contínua ainda sendo extremamente importante.

Definição 2.2.1. Seja x um número real. Definimos a parte inteira de x, pelo maior inteiro $\lfloor x \rfloor$ que não é maior do que x.

Assim, por exemplo $\lfloor 3 \rfloor = 3$, $\lfloor 3,7 \rfloor = 3$, $\lfloor -5,7 \rfloor = -6$. Como consequência da definição podemos escrever $x - 1 < \lfloor x \rfloor \leq x$ ou ainda $\lfloor x \rfloor \leq x < \lfloor x + 1 \rfloor$.

Teorema 2.2.1.(Algoritmo Euclidiano) Sejam a e b , inteiros, com $b \neq 0$. Existem q e r também inteiros, únicos, tais que $a = bq + r$, com $0 \leq r < b$. Estes inteiros q e r são chamados, respectivamente, quociente e resto da divisão de a por b.

Demonstração:

Seja $q = \lfloor \frac{a}{b} \rfloor$, pela definição acima, $\lfloor \frac{a}{b} \rfloor \leq \frac{a}{b} < \lfloor \frac{a}{b} \rfloor + 1 \Rightarrow b\lfloor \frac{a}{b} \rfloor \leq a < b\lfloor \frac{a}{b} \rfloor + b \Rightarrow bq \leq a < bq + b$. Temos, portanto que:

$$0 \leq a - bq \text{ e } a - bq < b.$$

Desta forma se definirmos $r = a - bq$, temos garantida a existência de q e r. Mostraremos agora a unicidade de q e r.

Suponha que existam outros valores distintos de q e r, chamemos estes outros valores de q_1 e r_1, respectivamente. Assim:

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

Então:

$qb + r = q_1 b + r_1 \Rightarrow b(q - q_1) = r_1 - r \Rightarrow b|(r_1 - r)$. Como $0 \leq r, r_1 < b$ temos que $|r_1 - r| < b$ então $|r_1 - r| = 0 \Rightarrow r_1 = r$ e consequentemente $q = q_1$. ■

2.3 Teorema Fundamental da Aritmética

Definição 2.3.1. Um número inteiro p $(p > 1)$, é dito primo se possui apenas dois divisores positivos 1 e p. Se $p > 1$ não é primo dizemos que p é *composto*.

Definição 2.3.2. Sendo m e n inteiros não simultaneamente nulos, diremos que d é um máximo divisor comum, *mdc*, e escrevemos (m, n), se

1. d é divisor comum m e n.
2. d é divisível por todo divisor comum de m e n.

Um importante resultado usado largamente quando trabalhamos com o máximo divisor comum é o lema abaixo descrito.

Lema 2.3.1.(Bézout[1]) Sejam a e b inteiros, existem x e y também inteiros tais que $(a, b) = ax + by$.

Demonstração:

Como qualquer divisor de x é também divisor de $-x$, para qualquer x inteiro, podemos então nos ater ao caso em que a e b são positivos. Assim, considere o conjunto $D = \{ax + by; x, y \in \mathbb{Z}\}$. D possui elementos estritamente positivos, por exemplo, $a + b$. Para tanto basta considerar $x = y = 1$. Seja d o menor elemento dentre os elementos estritamente positivos em D. Assim $d = ax+by$, para os inteiros x e y convenientes. Mostraremos que $d = (a, b)$. De fato, note que d > 0. Fazendo uso do Algoritmo de Euclides, temos:

$a = dq + r$, com $0 \leq r < d$, como $d = ax + by$ então: $a = (ax + by)q + r \Rightarrow a = axq + byq + r \Rightarrow a - axq - byq = r \Rightarrow a(1 - xq) + b(-yq) = r$ assim $r \in D$. Como d é o menor elemento positivo de D e $r < d$, r não pode ser estritamente positivo, logo $r = 0$. Assim $a = dq \Rightarrow d|a$. Analogamente chega-se que $d|b$. Consideremos d', tal que $d'|a$ e $d'|b$, então sendo x, y, k' e k inteiros, temos:

$d'|a \Rightarrow d'|xa \Rightarrow xa = kd'$ e $d'|b \Rightarrow d'|yb \Rightarrow yb = k'd'$, então $xa+yb = (k+k')d' \Rightarrow d'|(xa + yb)$ como $d = xa + yb$ temos que $d'|d$. Logo $d = (a, b)$. ■

Definição 2.3.3. Sejam m e n dois números inteiros positivos. Se o máximo divisor comum entre eles for igual a 1, dizemos que eles são primos entre si, isto é, $(m, n) = 1$.

Consequentemente podemos escrever que o $(m, n) = 1$ se, e somente se, existem inteiros x e y tais que $mx + ny = 1$.

Lema 2.3.2. Se p é primo e $p|ab$, com a e b inteiros, então $p|a$ ou $p|b$.

Demonstração:

Basta mostrar que, se $p|ab$ e $p \nmid a$, então $p|b$. Se $p \nmid a \Rightarrow (p, a) = 1$, pois p é primo. Pelo lema anterior existem x e y, inteiros, tais que $px + ay = 1$.

[1]Étiènne Bézout (1730 - 1783), matemático francês consagrado pela publicação da coleção *Cours de mathématique*.

Como $p|ab$, exite k, inteiro, tal que $ab = pk$. Assim:

$$px + ay = 1 \Rightarrow bpx + bay = b \Rightarrow p(bx + ky) = b \Rightarrow p|b.$$

Em particular, se a e b forem primos distintos, se $p|ab$, então $p = a$ ou $p = b$ ■

Proposição 2.3.1. Sejam a, b, c inteiros, $(ac, b) = 1 \Leftrightarrow (a, b) = (c, b) = 1$.

Demonstração:

Suponhamos $(ac, b) = 1$ então existem inteiros x e y tais que $(ac)x + (b)y = (c)ax + (b)y = (a)cx + (b)y = 1$ então $(a, b) = 1$ e ainda $(c, b) = 1$.
Por outro lado se $(a, b) = (c, b) = 1$, existem $x_{1,2}$ e y_1, y_2, inteiros tais que:

$$x_1a + y_1b = 1 \quad \text{e} \quad x_2c + y_2b = 1.$$

Assim:

$$(x_1a + y_1b)(x_2c + y_2b) = 1 \Rightarrow (x_1x_2)ac + (x_1ay_2 + y_1x_2c + y_1by_2)b = 1.$$

Portanto $(ac, b) = 1$. ■

Teorema 2.3.1.(Teorema Fundamental da Aritmética) Todo número inteiro maior do que 1 ou é primo ou se escreve de modo único (exceto pela ordem dos seus fatores) como produto de primos.

Demonstração:

Seja $n > 1$, inteiro, usando indução sobre n. Se $n = 2$ não há o que provar, pois n é primo. Supondo agora $2 \leq n \leq k$, onde k é um inteiro e n é produto de finitos primos, provaremos para k. Se k é primo não há nada a ser provado e a demonstração está terminada, porém, se k não é primo existem a e b inteiros, tal que $k = a.b$, onde $1 \leq a, b \leq k$, pela hipótese indutiva a e b podem ser escritos da forma:

$$a = \prod_{i=1}^{r} p_i$$

e

$$b = \prod_{j=1}^{s} q_i$$

onde p_i e q_j são números primos. Então:

$$k = \prod_{i=1}^{r} p_i . \prod_{j=1}^{s} q_i = p_1.p_2.p_3...p_r.q_1.q_2.q_3...q_s$$

portanto, escrito como produto finito de primos.

Provemos agora a unicidade da escrita. Suponha agora que $n = p_1.p_2.p_3...p_r$ e $n = q_1.q_2.q_3...q_s$, tal que p_i e q_j são primos e $p_i \neq q_j$. Então $p_1.p_2.p_3...p_r = q_1.q_2.q_3...q_s \Rightarrow p_1|(q_1.q_2.q_3...q_s) \Rightarrow p_1|q_j$ para algum $1 \leq j \leq s$, pelo lema acima $p_1 = q_j$, podemos supor $j = 1$. Assim $p_2.p_3...p_r = q_2.q_3...q_s$ e usando o mesmo argumento teremos $p_2 = q_2$,$p_3 = q_3$ e $p_r = q_s$ e portanto $r = s$. ■

Definição 2.3.4. Uma sequência de números reais é uma função $f : \mathbb{N} \longrightarrow \mathbb{R}$, que associa a cada $n \in \mathbb{N}$ um número real, este chamado de n-ésimo termo da sequência.

Escreve-se $(x_n)_{n\in\mathbb{N}}$ para indicar a sequência na qual o n-ésimo termo é x_n .Por exemplo a sequência $(x_n)_{n\in\mathbb{N}}$ onde $x_n = 2n$, ou seja, $(2, 4, 6, ...)$ que indica a sequência dos números pares, ou $x_n = (\frac{1}{n})^n$ que será $(1, \frac{1}{4}, \frac{1}{27}, ...)$.

Diante dos muitos exemplos de sequências existente nos vários ramos da matemática, podemos escrever uma sequência particularmente importante, a sequência dos números de Fermat,que será definida abaixo.

Definição 2.3.5. Seja $n \in \mathbb{N}$ os números da forma $2^{2^n} + 1$ são chamados Números de Fermat.

Assim a sequência $(F_n)_{n\in\mathbb{N}}$ onde $F_n = 2^{2^n}+1$ é formada pelos números de Fermat.

O matemático francês Pierre de Fermat (1601-1655) é famoso pelo seu extenso trabalho em aritmética. Muitos dos resultados e problemas deixados por Fermat motivaram um extraordinário avanço na Matemática. Falaremos então dos números de Fermat.

Em 1640 Fermat conjecturou, em uma de suas varias cartas, que estes números eram todos primos[2]. De fato, sendo $n = 0, 1, 2, 3$ e 4 , tem-se $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$, sendo estes todos números primos. Porém Euler em 1772, mostra que $F_5 = 4.294.967.297$ não é primo.

Vejamos um resultado importante sobre os números de Fermat.

[2]No Capítulo 3 mostraremos que $F(4)$ é primo e que $F(5)$ é composto e exibiremos um de seus divisores primo.

Lema 2.3.3. Um número de Fermat é igual ao produto de todos as anteriores mais 2, isto é, sendo $n \geq 0$ inteiro e F_n um número de Fermat então

$$F_n = 2 + \prod_{i=1}^{n-1} F_i.$$

Demonstração:

Sendo a proposição a ser provada $P(n)$, usaremos o método de indução sobre n.

Se $n = 1$ temos que $P(1)$ é verdade, pois $F_1 = 2^{2^1} + 1 = 5 = 3 + 2 = 2^{2^0} + 1 + 2 = F_0 + 2$ e portanto $F_1 = F_0 + 2$.

Suponhamos que $P(n)$ é verdadeira, ou seja, $F_n = 2 + \prod_{i=1}^{n-1} F_i$ para algum $n > 1$ inteiro.

Considere agora o número de Fermat $F_{n+1} = 2^{2^{n+2}} + 1$ então:

$F_{n+1} = 2^{2^{n+1}} + 1 = 2^{2^n.2} + 1 = (2^{2^n})^2 + 1 = (2^{2^n})^2 - 1 + 2 = [(2^{2^n})^2 - 1^2] + 2 = (2^{2^n}+1).(2^{2^n}-1)+2 = (2^{2^n}+1).(2^{2^n}+1-2)+2 = F_n(F_n-2)+2 = F_n.F_n - 2F_n + 2.$

Como $F_n = 2 + \prod_{i=1}^{n-1} F_i$, temos:

$$F_n.F_n - 2F_n + 2 = (2 + \prod_{i=1}^{n-1} F_1).F_n - 2F_n + 2 = 2F_n + \prod_{i=1}^{n} F_i - 2F_n + 2 = \prod_{i=1}^{n} F_i + 2.$$

Logo $F_{n+1} = \prod_{i=1}^{n} F_i + 2$. ■

Lema 2.3.4. Sejam n e m números inteiros positivos distintos então os números de Fermat F_n e F_m são primos entre si, isto é, $(F_n, F_m) = 1$.

Demonstração:

Suponha que $(F_n, F_m) \neq 1$, isto é, F_n e F_m têm um fator primo p em comum, portanto $p|F_n \Rightarrow p|F_0.F_1F_2...F_n...F_{m-1}$, suponha ainda, sem nenhuma perda de generalidade, que $n < m$, então pelo **Lema 2.3.3.** temos:

$F_m = F_0.F_1F_2...F_n...F_{m-1} + 2$ como $p|F_m \Rightarrow p|(F_0.F_1F_2...F_n...F_{m-1} + 2)$ então $p|(F_0.F_1F_2...F_n...F_{m-1}) \Leftrightarrow p|2$. Como $p|(F_0.F_1F_2...F_n...F_{m-1})$ então $p|2 \Rightarrow p = 2$.

Logo $2|F_m$ então F_m é par. Absurdo!

Portanto $(F_n, F_m = 1)$. ■

2.4 Congruências

Tratando-se do estudo das divisões euclidianas, quando se enfatiza os seus restos, o melhor instrumento a ser utilizado são as congruências. Introduzidas por Gauss em seu célebre trabalho "Disquisitiones Arithmeticae", de 1801, foram imediatamente adotadas pelos estudiosos da época e ainda são largamente utilizadas atualmente.

Nesta seção introduziremos a noção de congruências e algumas de suas propriedades.

Definição 2.4.1. Sejam a, b e n inteiros, com $n > 1$. Se $n|(a-b)$ diremos que a é congruente a b, módulo n, e escrevemos $a \equiv b \bmod n$. Caso contrário, diremos que a não é congruente a b módulo n ou seja $a \not\equiv b \bmod n$.

Por exemplo, de acordo com a definição acima temos que $5 \equiv 2 \bmod 3$, pois $3|(5-2)$, já $20 \not\equiv 17 \bmod 5$ pois $5 \nmid (20-17)$.

Proposição 2.4.1. Sejam a, b e n inteiros, com $n > 1$. $a \equiv b \bmod n$ se, e somente se, a e b deixam restos iguais na divisão por n.

Demonstração:

Suponha que $a \equiv b \bmod n$. Então, $n|(a-b)$. Pelo **Teorema 2.2.1.**, existem q_1, q_2, r_1, e r_2, univocamente determinados, tais que:

$a = nq_1 + r_1$ e $b = nq_2 + r_2$, com $0 \leq r_1, r_2 < n$ então $|r_1 - r_2| < n$. Assim $a - b = n(q_1 - q_2) + (r_1 - r_2)$. Como $n|(a-b)$, temos que $n|(r_1 - r_2)$. Portanto, a única possibilidade é $|r_1 - r_2| = 0 \Rightarrow r_1 = r_2$.

Por outro lado, sendo $a = nq_1 + r$ e $b = nq_2 + r$, com $0 \leq r < n$, temos $a - b = n(q_1 - q_2) + (r - r) = n(q_1 - q_2) \Rightarrow n|(a-b) \Rightarrow a \equiv b \bmod n$. ■

Note que, se a deixa resto r na divisão Euclidiana por n então $a \equiv r \bmod n$. Com efeito, pelo algoritmo de Euclides existem q e r inteiros, tais que, $a = nq + r$ com $0 \leq r < n$, assim $nq = (a - r) \Rightarrow a \equiv r \bmod n$. Como $0 \leq r < n$, isto é, r assume um dos valores $0, 1, 2, 3, ..., n-1$, tem-se que a é côngruo a um destes números.

Proposição 2.4.2. Sejam a, b, c, d e n inteiros, com $n > 1$, temos:

1. $a \equiv a \bmod n$;
2. Se $a \equiv b \bmod n$, então $b \equiv a \bmod n$;
3. Se $a \equiv b \bmod n$ e $b \equiv c \bmod n$, então $a \equiv c \bmod n$;
4. Se $a \equiv b \bmod n$ e $c \equiv d \bmod n$, então $a + c \equiv b + d \bmod n$;
5. Se $a \equiv b \bmod n$ e $c \equiv d \bmod n$, então $a.c \equiv b.d \bmod n$;
6. Se $(c, n) = 1$, então $ac \equiv bc \bmod n$ se, e somente se $a \equiv b \bmod n$.

Demonstração:

1. Sendo $n > 1$ então $n|0 \Rightarrow n|(a - a) \Rightarrow a \equiv a \bmod n$.

2. Se $a \equiv b \bmod n \Rightarrow n|(a - b) \Rightarrow n| - 1(b - a)$ como $n > 1$ temos que $n|(b - a) \Rightarrow b \equiv a \bmod n$.

3. Se $a \equiv b \bmod n$ e $b \equiv c \bmod n$ temos $n|(a-b)$ e $n|(c-d) \Rightarrow n|(a-b+c-d) \Rightarrow n|((a + c) - (b + d))$ portanto $a + c \equiv b + d \bmod n$.

4. Se $a \equiv b \bmod n$ e $b \equiv c \bmod n$ temos $n|(a - b)$ e $n|(c - d)$, assim $a - b = xn$ e $c - d = yn$, com x, y inteiros, então $(a - b) + (c - d) = xn + yn \Rightarrow (a + c) - (b + d) = n(x + y) \Rightarrow n|(a + c) - (b + d) \Rightarrow a + c \equiv b + d \bmod n$.

5. Se $a \equiv b \bmod n$ e $c \equiv d \bmod n$ então $a - b = xn$ e $c - d = yn$, com x, y inteiros, Como $ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b) = ayn + dxn = (ay + dx)n \Rightarrow n|(ac - bd)$, logo $ac \equiv bd \bmod n$.

6. Como $(c, n) = 1 \Rightarrow n \nmid c$, portanto $ac \equiv bc \bmod n \Leftrightarrow n|(ac - bc) = c(a - b) \Leftrightarrow n|(a - b) \Leftrightarrow a \equiv b \bmod n$ ■

Corolário 2.4.1. $a + c \equiv b + c \bmod n \Leftrightarrow a \equiv b \bmod n$.

Demonstração:

Se $a \equiv b \bmod n$, segue-se imediatamente que $a + c \equiv b + c \bmod n$ já que $c \equiv c \bmod n$, pelo item 4. da proposição anterior.

Por outro lado, suponhamos que $a + c \equiv b + c \bmod n$. Então $n|(a + c) - (b + c) = (a - b) \Rightarrow a \equiv b \bmod n$ ■

Teorema 2.4.1. Sejam a e n inteiros, com $n > 1$. Existe um inteiro x, tal que $ax \equiv 1 \bmod n$ se, e somente se, $(a, n) = 1$. Além disso y é uma solução da congruência se, e somente se, $x \equiv y \bmod n$.

Demonstração: Sendo $ax \equiv 1 \bmod n$ então $ax - 1 = yn$, com y inteiro. Assim $ax - yn = 1 \Rightarrow a(x) + n(-y) = 1$, pelo **Lema 2.3.1.**, $(a, n) = 1$. Por outro lado, sendo $(a, n) = 1$, e usando o **Lema 2.3.1.**, existem x e y inteiros, tais que, $ax + ny = 1 \Rightarrow ax - (-y)n = 1 \Rightarrow ax - 1 = yn \Rightarrow ax \equiv 1 \bmod n$.

Sendo y e x soluções de $ax \equiv 1 \bmod n$ temos que $ay \equiv 1 \bmod n$ e $1 \equiv ax \bmod n$, então $ay.1 \equiv 1.ax \bmod n \Rightarrow y \equiv x \bmod n$, pois a e n são primos ente si.

E ainda, se y é solução de $ax \equiv 1 \bmod n$ e $y \equiv x \bmod n$ temos que x também é solução da mesma congruência, pois $ax \equiv ay \equiv 1 \bmod n$ ■

2.5 A Infinitude dos Números Primos

Desde a antiguidade, problemas com relação a números primos têm fascinado os matemáticos. Gauss chegou a afirmar em um de seus trabalhos que "O problema de distinguir números primos de compostos e de decompor números compostos em fatores primos é conhecido como sendo um dos mais importantes e úteis da aritmética...".Embora não haja qualquer livro sobre este assunto por ele escrito, Euler escreveu diversas cartas e artigos sobre os vários aspectos desta teoria. Euclides de Alexandria propôs e provou, em sua grande obra *Elementos*, no livro IX, a seguinte afirmação:

"Existem infinitos números primos"

.

Nesta seção abordaremos os números primos. Estes que são as ferramentas principais da aritmética. Apesar de já termos visto a demonstração original de Euclides para esta afirmação, vale a pena demonstrarmos novamente no contexto dos primos de Fermat. É o que faremos no próximo teorema.

Teorema 2.5.1. A sequência $(p_n)_{n\in\mathbb{N}}$, onde p_n é primo, possui infinitos termos.

Demonstração:

Considere a sequência $(F_n)_{n\in\mathbb{N}}$ onde F_n é um número de Fermat. Suponha que p_1 é um fator primo de F_1 , p_2 é um fator primo de F_2 e p_n é um fator primo de

F_n , como $F_n < F_{n+1}$ e pelo **Lema 2.3.4.**, $(F_i, F_j) = 1$ com $i \neq j$ e $i, j \in \mathbb{N}$, então $(p_i, p_j) = 1$ e $(p_n)_{n\in\mathbb{N}}$ é infinita já que F_n é infinita. ■

Provamos portanto que existem infinitos números primos.

Muitos dos problemas mais famosos da matemática estão diretamente ligados a aritmética, em particular aos números primos. Alguns desses problemas ainda não foram resolvidos enquanto outros só foram resolvidos com sofisticadas ferramentas e outros até com o surgimento de novas áreas de estudo na matemática.

Definição 2.5.1. Seja a função $\pi : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $\pi(x)$ é o número de primos positivos menores ou iguais a x, isto é, $\pi(x)$ é quantidade de primos p que satisfazem a condição $2 \leq p \leq x$.

Assim, por inspeção direta consegue-se calcular alguns valores para $\pi(x)$, por exemplo $\pi(10) = 4$, pois os números primos no intervalo $[2, 10]$ são 2, 3, 5 e 7. Sendo x um valor muito grande é totalmente impossível determinar $\pi(x)$, assim o **Teorema 2.5.1.** pode ser escrito da seguinte maneira:

Teorema 2.5.1'

$$\lim_{n\longrightarrow\infty} \pi(n) = \infty$$

Introduziremos a notação $f(x) \sim g(x)$ para indicar que as funções f e g, contínuas de valores reais positivos, são assintoticamente iguais quando x tende para infinito, isso é $\lim\limits_{x\longrightarrow\infty} \dfrac{f(x)}{g(x)} = 1$.

Em 1792, Gauss, conjecturou que $\pi(x)$ era assintoticamente igual à função integral logarítmica, definida como:

$$Li(x) = \int_2^x \frac{1}{\ln t} dt$$

Sendo $Li(x) \sim \dfrac{x}{\ln x}$ podemos escrever que

$$\pi(x) \sim \frac{x}{\ln x}.$$

Observando a tabela[3] abaixo veremos alguns valores de $\pi(x)$ e também, evidências numéricas da apriximação de valores, entre $Li(x)$ e $\dfrac{x}{\ln x}$.

x	$\pi(x)$	$Li(x)$	$x/\ln x$
10^3	168	178	145
10^4	1.229	1.246	1.086
10^5	9.592	9.630	8.686
10^6	78.498	78.628	72.382
10^7	664.579	664.918	620.421
10^8	5.761.455	5.762.209	5.428.681
10^9	50.847.534	50.849.235	48.284.942
10^{10}	455.052.511	455.055.615	434.294.481
10^{11}	4.118.054.813	4.118.066.401	3.948.131.653
10^{12}	37.607.912.018	37.607.950.281	36.191.206.825

Gaus foi incapaz de provar suas conjecturas. Um grande passo na direção da demonstração desta afirmação foi da por Tchebychev[4] que, em 1852, demonstrou que existem constantes a e b, $0 < a < 1 < b$ com $x \geq 2$, tais que,

$$a\frac{x}{lnx} < \pi(x) < b\frac{x}{lnx}.$$

Ele provou também que se o limite

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x}$$

existe, então seu valor deve ser 1. O fim dessa parte da história veio com o *Teorema dos Números Primos*. Este teorema só foi demonstrado completamente por de *la Vallèe Poussin*[5] e *Hadamard*[6] (independentemente), por volta de 1900, mas baseados nas ideias de Riemann. Eles provaram a existência desse limite e desse modo completaram a prova do Teorema dos Números Primos:

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

[3]Para mais valores de x, $Li(x) - \pi(x)$ e $(x/\ln x) - \pi(x)$, consultar [11]

[4]Pafnuti Lvovitch Tchebychev (Okatowo, circunscrição de Borovsk, perto de Moscou, 4 de maio/16 de maio de 1821 - São Petersburgo, 26 de novembro/8 de dezembro de 1894) foi um matemático russo.

[5]Charles-Jean Étienne Gustave Nicolas de la Vallée Poussin (Lovaina, 14 de agosto de 1866 - 2 de março de 1962) foi um matemático belga.

[6]Jacques Salomon Hadamard (Versalhes, 8 de dezembro de 1865 - Paris, 17 de outubro de 1963) foi um matemático francês.

Além disso, podemos fazer uma afirmação sobre a magnitude do n-ésimo primo, ou seja uma cota superior para p_n, com p primo.

Afirmação 2.5.1. Para o n-ésimo primo p_n vale a estimativa

$$p_n \leq 2^{2^{n-1}}$$

Demonstração:

Seja $P(n)$ a afirmação a ser provada, usaremos indução sobre n. Temos que $P(1)$ é verdade, já que $2^{2^{1-1}} = 2^{2^0} = 2^1 = 2 = p_1$. Suponhamos que $P(n)$ é verdadeira.

Considere o número inteiro $k = p_1p_2p_3...p_n + 1$ e seja d um divisor de k, então $d \neq p_i$ com $1 \leq i \leq n$ e $d \leq k$, portanto $d > p_n$ em particular $d \geq p_{n+1}$. Assim $p_{n+1} \leq k$, pela hipótese indutiva temos que:

$p_1p_2p_3...p_n + 1 = 2^{2^0}2^{2^1}2^{2^2}...2^{2^{n-1}} + 1 = 2^{2^0+2^1+2^2+...2^{n-1}} + 1 = 2^{2^n-1} + 1 \leq 2^{2^n-1} + 2^{2^n-1} = 2^{2^n}$.

Portanto $p_{n+1} \leq 2^{2^n}$. ■

Sabemos que é possível escrever sequências, arbitrariamente grandes, de naturais que são formadas apenas por números compostos. Mostraremos a veracidade desta afirmação na **Proposição 2.5.2** abaixo, antes porém, necessitamos de alguns resultados prévios.

Definição 2.5.2 seja n um número inteiro não negativo, definimos o fatorial de n, e indicamos $n!$, como $n! = \prod_{i=1}^{n} i$. Definiremos ainda que $0! = 1! = 1$.

Proposição 2.5.1 Seja m um inteiro positivo, tal que $2 \leq m < n + 1$. Então $m|(n + 1)! + m$.

Demonstração:

Se então $2 \leq m < n + 1 \Rightarrow (n + 1)! = (n + 1).n.(n - 1)...m...3.2.1 \Rightarrow m|(n + 1)!$ como $m|m$ temos $m|[(n + 1)! + m]$, pela propriedade (4). da divisibilidade. ■

Proposição 2.5.2. Para todo número natural $n \geq 2$, existem n números naturais consecutivos compostos.

Demonstração:

Considere a sequencia $(a_k)_{k\in\mathbb{N}}$ definida por $a_k = (n+1)! + k$, com $k \leq n+1$ pela **Proposição 2.5.1.** $k|a_k$ para qualquer $n \geq 2$. Portanto a sequencia $(a_k)_{k\in\mathbb{N}}$ é formada por números compostos. ■

Mesmo como mostra a proposição acima, é possível demostrar que os números primos não estão tão espaçados assim. É o que prova o **Teorema 2.6.1.**. Para tanto, precisaremos dos seguintes resultados.

Proposição 2.5.3. Seja n um número natural e p um primo. Então a maior potência de p que divide $n!$ é p^k, onde

$$k = \lfloor\frac{n}{p}\rfloor + \lfloor\frac{n}{p^2}\rfloor + \lfloor\frac{n}{p^3}\rfloor + ...$$

Note que a soma acima é finita, pois, para algum natural r, teremos $n < p^r \Rightarrow \lfloor\frac{n}{p^r}\rfloor = 0$.

Demonstração:

Seja α o maior expoente de p que divide $n!$. Note que no produto $1.2.3...(n-1).n = n!$ apenas os múltiplos de p contribuem com um fator. Há $\lfloor\frac{n}{p}\rfloor$ tais múltiplos entre 1 e n. Destes, os que são múltiplos de p^2 contribuem com um fator p a mais, e há $\lfloor\frac{n}{p^2}\rfloor$ destes fatores. Dentre estes últimos, os que são múltiplos de p^3 contribuem com mais um fator p e destes existem $\lfloor\frac{n}{p^3}\rfloor$, e assim por diante. Assim temos que $\alpha = \lfloor\frac{n}{p}\rfloor + \lfloor\frac{n}{p^2}\rfloor + \lfloor\frac{n}{p^3}\rfloor + ...$ ■

Definição 2.5.3. Sejam n e k números inteiros positivos, tais que $n \geq k$. Definimos $\begin{pmatrix} n \\ k \end{pmatrix}$ como número binomial, onde $\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k!.(n-k)!}$. Temos ainda que:

$$\begin{pmatrix} n \\ k \end{pmatrix} = \begin{cases} 1, & se \quad k = n \quad ou \quad k = 0 \\ n, & se \quad k = 1 \\ 0 & se \quad k > n \end{cases}$$

Proposição 2.5.4. Sejam n, k inteiros positivos tais que $n \geq 2$ e $n \geq k$, temos que:

1. $\left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) + \left(\begin{array}{c} n-1 \\ k \end{array} \right) = \left(\begin{array}{c} n \\ k \end{array} \right)$ (Relação de Stifel[7]);

2. $\sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) = 2^n$.

Demonstração:

1. Temos

$$\left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) = \frac{(n-1)!}{[(n-1)-(k-1)]!(k-1)!} = \frac{(n-1)!}{(n-k)!(k-1)!}$$

e

$$\left(\begin{array}{c} n-1 \\ k \end{array} \right) = \frac{(n-1)!}{[(n-1)-k]!k!} = \frac{(n-1)!}{[(n-k)-1]!k(k-1)!}, \text{ portanto:}$$

$$\left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) + \left(\begin{array}{c} n-1 \\ k \end{array} \right) = \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{[(n-k)-1]!k(k-1)!} =$$

$$= (n-1)! \left(\frac{1}{(n-k)!(k-1)!} + \frac{1}{[(n-k)-1]!k(k-1)!} \right) = (n-1)! \frac{(n-k)+k}{(n-k)!k(k-1)!} =$$

$$\frac{n(n-1)!}{(n-k)!k!} = \frac{n!}{(n-k)!k!} = \left(\begin{array}{c} n \\ k \end{array} \right).$$

2.Usaremos indução sobre n. Temos que proposição $P(n)$, a ser provada, é verdade quando $n = 1$, pois $\sum_{k=0}^{2} \left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} 2 \\ 0 \end{array} \right) + \left(\begin{array}{c} 2 \\ 1 \end{array} \right) + \left(\begin{array}{c} 2 \\ 2 \end{array} \right) = 1+2+1 = 4 = 2^2$.

Suponhamos agora $P(n)$ verdadeira, mostraremos que $P(n+1)$ é verdade.

Consideremos a seguinte soma $\sum_{k=0}^{n+1} \left(\begin{array}{c} n+1 \\ k \end{array} \right) = \left(\begin{array}{c} n+1 \\ 0 \end{array} \right) + \sum_{k=1}^{n} \left(\begin{array}{c} n+1 \\ k \end{array} \right) +$

$\left(\begin{array}{c} n+1 \\ n+1 \end{array} \right)$, pelo item anterior:

[7]Michael Stifel, ou ainda Styfel, Stieffel, Stiefel, (Esslingen, 1487 - Jena, 19 de Abril de 1567) foi um matemático alemão.

$$\sum_{k=0}^{n+1}\left(\begin{array}{c} n+1 \\ k \end{array}\right) = 1+\sum_{k=1}^{n}\left(\left(\begin{array}{c} n \\ k \end{array}\right)+\left(\begin{array}{c} n \\ k-1 \end{array}\right)\right)+1 = 1+\sum_{k=1}^{n}\left(\begin{array}{c} n \\ k \end{array}\right)+\sum_{k=1}^{n}\left(\begin{array}{c} n \\ k-1 \end{array}\right)+$$
$$1 = \left(\begin{array}{c} n \\ 0 \end{array}\right)+\sum_{k=1}^{n}\left(\begin{array}{c} n \\ k \end{array}\right)+\sum_{k=1}^{n}\left(\begin{array}{c} n \\ k-1 \end{array}\right)+\left(\begin{array}{c} n \\ n \end{array}\right) = \sum_{k=0}^{n}\left(\begin{array}{c} n \\ k \end{array}\right)+\sum_{k=1}^{n+1}\left(\begin{array}{c} n \\ k-1 \end{array}\right) =$$
$$\sum_{k=0}^{n}\left(\begin{array}{c} n \\ k \end{array}\right)+\sum_{j=o}^{n}\left(\begin{array}{c} n \\ j \end{array}\right) = 2^n + 2^n = 2.2^n = 2^{n+1}. \blacksquare$$

Como consequência do item 2. podemos escrever a seguinte relação:

$$\left(\begin{array}{c} 2n \\ 0 \end{array}\right)+\left(\begin{array}{c} 2n \\ 1 \end{array}\right)+\left(\begin{array}{c} 2n \\ 2 \end{array}\right)+...+\left(\begin{array}{c} 2n \\ k \end{array}\right)+\left(\begin{array}{c} 2n \\ k+1 \end{array}\right)+...+\left(\begin{array}{c} 2n \\ 2n \end{array}\right) = 2^{2n}.$$

Portanto, para todo $0 \leq k \leq 2n-1$, vale que:

$$\left(\begin{array}{c} 2n \\ k \end{array}\right)+\left(\begin{array}{c} 2n \\ k+1 \end{array}\right) < 2^{2n}. \tag{2.1}$$

Lema 2.5.1. Seja n um número natural e p um número primo. Seja k um inteiro tal que $p^k \leq 2n \leq p^{k+1}$. Então o expoente de maior potência de p que divide $\left(\begin{array}{c} 2n \\ n \end{array}\right)$ é menor ou igual a k.

Demonstração:

Considere o número binomial $\left(\begin{array}{c} 2n \\ n \end{array}\right)$, sendo r e s os expoentes das maiores potências de p que dividem $(2n)!$ e $n!$, respectivamente. Temos, pela **Proposição 2.3.3.** que:

$$r = \lfloor\frac{2n}{p}\rfloor + \lfloor\frac{2n}{p^2}\rfloor + \lfloor\frac{2n}{p^3}\rfloor + ...$$

e

$$s = \lfloor\frac{n}{p}\rfloor + \lfloor\frac{n}{p^2}\rfloor + \lfloor\frac{n}{p^3}\rfloor + ...$$

como $\left(\begin{array}{c} 2n \\ n \end{array}\right) = \frac{(2n)!}{n!n!} = (2n)!(n!)^{-2}$,$p^r|(2n)!$ e $p^s|n!$, temos que o expoente da

maior potência que divide $\binom{2n}{n}$ é $r-2s$. Pela hipótese $p^k \leq 2n$, temos

$$r = \lfloor \frac{2n}{p} \rfloor + \lfloor \frac{2n}{p^2} \rfloor + ... + \lfloor \frac{2n}{p^k} \rfloor \quad \text{e} \quad s = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + ... + \lfloor \frac{n}{p^k} \rfloor.$$

Então

$$r - 2s = \sum_{i=1}^{k} \left(\lfloor \frac{2n}{p^i} \rfloor - 2\lfloor \frac{n}{p^i} \rfloor \right).$$

Pela **Definição 2.2.1.**, $\frac{n}{p^i} - 1 < \lfloor \frac{n}{p^i} \rfloor \leq \frac{n}{p^i} \Rightarrow -2\left(\frac{n}{p^i} - 1\right) > -2\lfloor \frac{n}{p^i} \rfloor \geq -2\frac{n}{p^i} \Rightarrow \frac{-2n}{p^i} - 2 > -2\lfloor \frac{n}{p^i} \rfloor \geq \frac{-2n}{p^i}$ e $\frac{2n}{p^i} - 1 < \lfloor \frac{2n}{p^i} \rfloor \leq \frac{2n}{p^i}$ assim:

$$\frac{-2n}{p^i} - 2 > -2\lfloor \frac{n}{p^i} \rfloor \geq \frac{-2n}{p^i} \tag{2.2}$$

e

$$\frac{2n}{p^i} \geq \lfloor \frac{2n}{p^i} \rfloor > \frac{2n}{p^i} - 1 \tag{2.3}$$

De 2.2 e 2.3, obtemos:

$\frac{-2n}{p^i} + 2 + \frac{2n}{p^i} > \lfloor \frac{2n}{p^i} \rfloor - 2\lfloor \frac{n}{p^i} \rfloor > \frac{-2n}{p^i} + \frac{2n}{p^i} - 1 \Rightarrow 2 > \lfloor \frac{2n}{p^i} \rfloor - 2\lfloor \frac{n}{p^i} \rfloor > -1.$

Então $\lfloor \frac{2n}{p^i} \rfloor - 2\lfloor \frac{n}{p^i} \rfloor$ assume somente dois valores: 0 e 1.

Portanto $r - 2s \leq \sum_{i=1}^{k} 1 = k$.

Em particular, se $p > \sqrt{2n}$ então o expoente máximo dessa potência de p é menor ou igual a 1. Com efeito, pois se $p \leq 2n < p^2$, isto é $k = 1$.

Além disso, se $\frac{2}{3}n < p < n$ então $p \nmid \binom{2n}{n}$. Com efeito, se $\frac{2}{n}n < p < n$, então p aparece uma vez na fatoração de $n!$, e duas vezes na fatoração de $2n!$, pois $\frac{2}{3}n < p \Rightarrow \frac{2n}{p} < 3$. Logo, como $\binom{2n}{n} = \frac{(2n)!}{n!n!}$, segue-se que a maior potência de

p em $\begin{pmatrix} 2n \\ n \end{pmatrix}$ é $2 - 2.1 = 0$ ■

Lema 2.5.2. Seja $n \geq 2$ inteiro positivo e p primo, então $\prod_{p \leq n} p < 4^n$.

Demonstração:

Esta demonstração será feita por indução sobre n. Sendo $P(n)$ a proposição a ser provada. Fica evidente que $P(n)$ é verdade se $n = 1$, 2 e 3.

Note que se $P(2m+1)$, para $m \geq 2$, é verdade então $P(2m+2)$ também será, pois $\prod_{p \leq 2m+2} p = \prod_{p \leq 2m+1} p < 4^{2m+1} < 4^{2m+2} \Rightarrow \prod_{p \leq 2m+2} p < 4^{2m+2}$, pois não agregamos novos primos ao produto, quando passamos de $2m+1$ a $2m+2$, logo basta provar a desigualdade para um valor ímpar $n = 2m+1$, isto é, provaremos que $P(2m+1)$ é verdadeira.

Assumindo que $P(m+1)$ seja verdadeira, temos que $\prod_{p \leq m+1} p < 4^{m+1}$.

Como todo primo no intervalo $(m+1) < p \leq (2m+1)$ é um fator de $\begin{pmatrix} 2m+1 \\ m+1 \end{pmatrix}$, pois p divide $(2m+1)!$ mas não divide $(m+1)!$ e nem $m!$, então:

$$\prod_{(m+1)<p\leq(2m+1)} p \leq \begin{pmatrix} 2m+1 \\ m+1 \end{pmatrix}.$$

De 2.1 temos:

$$\prod_{(m+1)<p\leq(2m+1)} p < 2^{2m} = 4^m.$$

Como $\prod_{p \leq m+1} p < 4^{m+1}$,temos :

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p. \prod_{(m+1)<p\leq(2m+1)} p < 4^{m+1}.4^m = 4^{2m+1}.$$

Portanto $\prod_{p \leq 2m+1} p < 4^{2m+1}$. ■

2.6 Postulado de Bertrand

Embora que tenhamos afirmado, e demonstrado, na **Proposição 2.5.2.**, que para todo número natural $n \geq 2$, existem n números naturais consecutivos compostos, os números primos não estão tão afastados assim, como mostra o teorema abaixo.

Teorema 2.6.1.(Postulado de Bertrand[8]) Seja n um número inteiro positivo. Então sempre existe um p primo, tal que $n \leq p \leq 2n$.

Demonstração:

Claramente essa afirmação é verdade para $n \leq 4$. Suponhamos que essa afirmação seja falsa para algum $n > 4$ e obteremos uma contradição.

Pela nossa suposição não há primos entre n e $2n$. Pelo **Lema 2.5.1.**, $p \nmid \binom{2n}{n}$ se $\frac{2}{3}n < p < n$, portanto $\binom{2n}{n} = \prod_{p \leq \frac{2n}{3}} p^k$. Seja p um primo e k o valor máximo tal que $p^k | \binom{2n}{n}$. Temos que $p^k \leq 2n$ e, se $p > \sqrt{2n}$, então $k \leq 1$. Assim:

$$\binom{2n}{n} = \prod_{p \leq \sqrt{2n}} p^k \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^k \leq \prod_{p \leq \sqrt{2n}} 2n \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p.$$

Pelo **lema 2.5.2.** temos agora:

$$\binom{2n}{n} \leq (2n)^r 4^{2n/3}, \tag{2.4}$$

com $1 \leq r \leq \sqrt{2n}$.

Sabemos que $2^n = \sum_{i=0}^{n} \binom{n}{i} \Rightarrow 2^{2n-1} = \binom{2n-1}{0} + \binom{2n-1}{1} + ... + \binom{2n-1}{n-1} + \binom{2n-1}{n} + ... + \binom{2n-1}{2n-1} < n\binom{2n-1}{n-1} + n\binom{2n-1}{n}$.

[8]Chamado assim apenas por razões históricas, pois foi demonstrado por Tchebychev.

Portanto:

$$2^{2n-1} < n\begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} + n\begin{pmatrix} 2n-1 \\ n \end{pmatrix} \Rightarrow \frac{2^{2n-1}}{n} < \begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} + \begin{pmatrix} 2n-1 \\ n \end{pmatrix}$$

Pelo item (1) da **Proposição 2.5.4.**. $\begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} + \begin{pmatrix} 2n-1 \\ n \end{pmatrix} = \begin{pmatrix} 2n \\ n \end{pmatrix}$ então:

$$\frac{2^{2n-1}}{n} < \begin{pmatrix} 2n \\ n \end{pmatrix}. \tag{2.5}$$

De 2.4 e 2.5 temos:

$$\frac{2^{2n-1}}{n} < (2n)^r 4^{2n/3}.$$

Consideremos um valor de n, satisfatório, de modo que $r = \sqrt{\frac{n}{2}} - 1$, $n = 100$ é suficiente, pois de 1 a 100 metade dos números são pares, e para valores maiores que 100 a hipótese se cumprirá, portanto:

$$\frac{2^{2n-1}}{n} < (2n)^{\sqrt{n/2}-1} 4^{2n/3} \Rightarrow \frac{2^{2n}}{2n} < \frac{(2n)^{\sqrt{n/2}}}{2n} 2^{4n/3} \Rightarrow 2^{2n/3} < (2n)^{\sqrt{n/2}}.$$

Aplicando o logaritmo, na base 2, temos:

$$\frac{2n}{3}\log_2 2 < \frac{\sqrt{n}}{\sqrt{2}}(\log_2 2 + \log_2 n) \Rightarrow \frac{2\sqrt{2}}{3}\sqrt{n} < 1 + \log_2 n.$$

Note que, pelo gráfico abaixo que a desigualdade anterior é falsa se $n \geq 50$.

Logo o teorema é válido se $n > 100$, resta-nos portanto verificar sua validade para $1 \leq n \leq 100$. Vejamos:

Se

$$1 \leq n \leq 2 \Rightarrow n \leq 2 \leq 2n$$

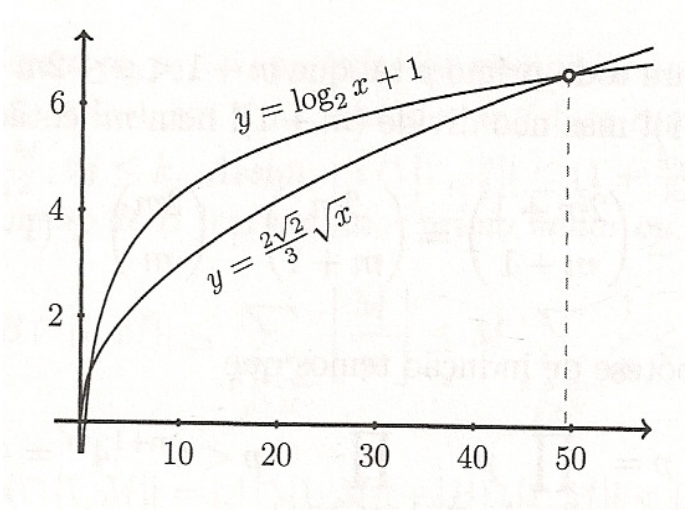

Figura 2.1:

$$3 \leq n \leq 5 \Rightarrow n \leq 5 \leq 2n$$
$$6 \leq n \leq 11 \Rightarrow n \leq 11 \leq 2n$$
$$12 \leq n \leq 23 \Rightarrow n \leq 23 \leq 2n$$
$$24 \leq n \leq 47 \Rightarrow n \leq 47 \leq 2n$$
$$48 \leq n \leq 79 \Rightarrow n \leq 79 \leq 2n$$
$$80 \leq n \leq 100 \Rightarrow n \leq 101 \leq 2n$$

Que completa a demonstração. ■

Apesar de ser uma afirmação simples e aparentemente elementar, a demonstração, como se viu, é bastante elaborada e engenhosa, além de bela!

Na **Afirmação 2.5.1.** mostramos uma cota superior para o n-ésimo primo. Aplicando a teorema acima podemos determinar uma nova estimativa.

Afirmação 2.6.1. Sendo p_n o n-ésimo primo, vale a estimativa:

$$p_n \leq 2^n.$$

Demonstração:

Seja $P(n)$ a propriedade a ser provada, se $n = 1$ temos $p_1 = 2 \leq 2^1$. Suponhamos que $P(n)$ é verdadeira.

Pelo **Teorema 2.3.2.** e usando a hipótese indutiva, teremos:

$$p_n \leq p_{n+1} \leq 2p_n \Rightarrow p_{n+1} \leq 2.2^n = 2^{n+1}.$$

Portanto $p_{n+1} \leq 2^{n+1}$. ■

Capítulo 3

Testes de Primalidade

Neste capítulo mostraremos três resultados para determinar se uma número é primo ou não. Abordaremos O Crivo de Eratóstenes, o Pequeno Teorema de Fermat e o Teorema de Wilson. Estes são ferramentas importantes e básicas da Teoria dos Números.

3.1 O Crivo de Eratóstenes

Como foi mostrado no **Teorema 2.5.1.**, existem infinitos números primos. Uma pergunta que naturalmente deriva desta afirmação é: *Como se pode obter uma lista contendo os números primos até uma determinada ordem?*

Um dos métodos mais antigos para elaborar tabelas de números primos é devido ao matemático grego Eratóstenes. Abaixo enunciaremos na proposição este método.

Proposição 3.1.1. Se um número $n > 1$, inteiro, for composto, então existe um divisor primo p de n, tal que $p^2 \leq n$.

Demonstração:

Seja $n > 1$ um número inteiro composto, então existem a, b, também inteiros, tal que $n = a.b$, com $1 < a \leq b$. Seja p um divisor de a, consequentemente um divisor de n, então:

$$p \leq a \Rightarrow p^2 \leq pa \leq a.a \leq ab = n.$$

Portanto $p^2 \leq n$. ■

Podemos fazer uso da proposição acima para mostrar, por exemplo, que o número 109 é primo. Vejamos:

Notemos inicialmente que $10 \leq \sqrt{109} \leq 11$. Portanto se 109 for composto, segue pela proposição acima que 109 deve possuir um divisor primo p, menor que 10, ou seja, $p \in \{2, 3, 5, 7\}$, podemos notar facilmente que 109 não é divisível por nenhum dos primos citados (basta usar o Algoritmo Euclidiano). Logo 109 é primo.

3.2 Pequeno Teorema de Fermat

Uma outra maneira de se saber se um determinado número é primo ou não, é usando o seguinte resultado, proposto por Fermat que afirma:

Seja $n > 1$, um inteiro positivo, se existir algum a, também inteiro positivo, com $(a, n) = 1$, tal que n não divide $(a)^{n-1} - 1$ então n não é primo.

A generalização desse fato, feita mais tarde por Euler terminando no Teorema de Euler, nos dá vários resultados, como por exemplo, a forma dos divisores primos dos números de Fermat.

A afirmação feita acima deriva do teorema que será demonstrado abaixo, para tanto, precisamos dos resultados que seguem.

Lema 3.2.1. Seja p um número primo. Então $p| \begin{pmatrix} p \\ k \end{pmatrix}$ onde $0 \leq k \leq p$.

Demonstração:

Se $k = 1$, é trivial que $p| \begin{pmatrix} p \\ k \end{pmatrix}$, pois $\begin{pmatrix} p \\ 1 \end{pmatrix} = p$.

Se $k \neq 1$, temos que $k!|k!. \begin{pmatrix} p \\ k \end{pmatrix}$.

Como $\begin{pmatrix} p \\ k \end{pmatrix} = \dfrac{p!}{k!(p-k)} = \dfrac{p(p-1)(p-2)...(p-(k-1))}{k!}$, então:

$$k!|(p-1)(p-2)...(p-(k-1)).$$

Note que $(k!, p) = 1$. Pois se $(k!, p) \neq 1 \Rightarrow p|k$, pois p é primo, e portanto

$$k! = 1.2.3...p...(k-1).k \Rightarrow p < k$$

contrariando o fato de que $0 \leq k \leq p$.

Então $k!|(p-1)(p-2)...(p-(k-1))$.

Temos que

$$\frac{(p-1)(p-2)...(p-(k-1))}{k!}$$

é um número inteiro positivo.

Logo

$$p|p\frac{(p-1)(p-2)...(p-(k-1))}{k!} \Rightarrow p|\frac{p!}{k!(p-k)!} \Rightarrow p|\left(\begin{array}{c} p \\ k \end{array}\right). \blacksquare$$

Teorema 3.2.1.(Pequeno Teorema de Fermat) Seja p um número primo, então $n^p \equiv n \bmod p$, para todo n inteiro positivo.

Demonstração:

Provaremos o teorema por indução sobre n. Consideremos a propriedade $P(n)$ a ser provada, $P(1)$ é verdade já que se $n = 1$, o resultado é óbvio! Pois $n^p - n = 1^p - 1 = 0$ e $n|o$, para todo n inteiro positivo. Suponhamos que $P(n)$ é valida, isto é, $p|(n^p - n)$. E provaremos a veracidade de $P(n+1)$.

Pelo desenvolvimento binomial temos: $(n+1)^p = \sum_{i=0}^{p} \left(\begin{array}{c} p \\ i \end{array}\right) n^{p-i}$.

Considere a sentença $(n+1)^p - (n+1) = \sum_{i=0}^{p} \left(\begin{array}{c} p \\ i \end{array}\right) n^{p-i} - (n+1) = n^p + \left(\begin{array}{c} p \\ 1 \end{array}\right) n^{p-1} + \left(\begin{array}{c} p \\ 2 \end{array}\right) n^{p-2} + ... + \left(\begin{array}{c} p \\ p-1 \end{array}\right) n^1 + 1 - n - 1 = (n^p - n) + [\left(\begin{array}{c} p \\ 1 \end{array}\right) n^{p-1} + \left(\begin{array}{c} p \\ 2 \end{array}\right) n^{p-2} + ... + \left(\begin{array}{c} p \\ p-1 \end{array}\right) n]$.

Usando o lema anterior e a hipótese indutiva, temos:

$p|\left(\begin{array}{c} p \\ 1 \end{array}\right) n^{p-1} + \left(\begin{array}{c} p \\ 2 \end{array}\right) n^{p-2} + ... + \left(\begin{array}{c} p \\ p-1 \end{array}\right) n$ e $p|(n^p - n)$, então:

$p|(n+1)^p + (n+1)$ $\blacksquare$

Definição 3.2.1. Seja m um inteiro positivo, o conjunto dos inteiros $\{r_1, r_2, ..., r_k\}$ é um *Sistema Completo de Resíduos* módulo m se:

1. $r_i \not\equiv r_j \bmod m$ para $i \neq j$ com $i, j = 1, 2, 3, ..., k$;
2. para todo inteiro n existe um r_i tal que $n \equiv r_i \bmod m$ com $i = 1, 2, 3, ..., k$.

Por exemplo $\{0, 1, 2, ..., m-1\}$ é um sistema completo de resíduos módulo m.

Se considerarmos um Sistema Completo de Resíduos módulo m e excluirmos deste conjunto os elementos que não são primos com m teremos um Sistema Reduzido de Resíduos, por exemplo $\{0, 1, 2, ...7\}$ formam um sistema completo de resíduos módulo 8, então se retirarmos desse conjunto os elementos que não são primos com 8 teremos o seguinte conjunto $\{1, 3, 5, 7\}$ que será um sistema reduzido de resíduos, portanto cabe a seguinte definição

Definição 3.2.2. Sendo m um inteiro positivo, $\{r_1, r_2, ..., r_k\}$ será um *Sistema Reduzido de Resíduos* módulo m se:

1. $(r_i, m) = 1$, para todo $i = 1, 2 = 3, ..., k$;
2. $r_i \not\equiv r_j \bmod m$ para $i \neq j$ com $i, j = 1, 2, 3, ..., k$

Definição 3.2.3. Seja $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ uma função, tal que para cada n natural associa-se a quantidade de números naturais menores que n que são primos com n. Assim pode-se escrever que $\varphi(n) = \#\{k \in \mathbb{N}; k < n \ e \ (k, n) = 1\}$, onde $\#$ indica o número de elementos do conjunto, tal função chama-se *A função fi de Euler*.

Assim, por exemplo, $\varphi(3) = 3$, $\varphi(10) = 4$, etc. A função fí de Euler é de grande utilidade em Teoria dos Números.

Proposição 3.2.1. Seja $\{r_1, r_2, ..., r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m e a um inteiro tal que $(a, m) = 1$, então $\{ar_1, ar_2, ..., ar_{\varphi(m)}\}$ é também um sistema reduzido de resíduos módulo m.

Demonstração:

Note que $(ar_i, m) = 1$ para $i = 1, 2, 3, ..., \varphi(m)$. De fato, pois r_i e a não possuem fatores primos com m e portanto ar_i também não possui, logo $(ar_i, m) = 1$, com $i = 1, 2, 3, ..., \varphi(m)$.

Suponhamos agora que $ar_i \equiv ar_j \bmod m$, com $i \neq j$, como $(a, m) = 1$ temos $r_i \equiv r_j \bmod m$. Absurdo! Pois $\{r_1, r_2, ..., r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m.

Logo $\{ar_1, ar_2, ..., ar_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m ■

Proposição 3.2.2. Sejam a, q e m inteiros, com $m > 1$ e $(k, m) = 1$. Se $r_1, r_2, ..., r_k$ um sistema completo de resíduos módulo m, então

$$a + qr_1, a + qr_2, ..., a + qr_k$$

é também um sistema completo de resíduos módulo m.

Demostração:

Sejam $i, j = 0, 1, 2, 3, ..., m-1$, pelo item (6). da **Proposição 2.4.2.** e o **Corolário 2.4.1.**, temos:
$a + qr_i \equiv a + qr_j \bmod m \Leftrightarrow qr_i \equiv qr_j \bmod m \Leftrightarrow r_i \equiv r_j \bmod m \Leftrightarrow i = j$.

Isso nos mostra que $a + qr_1, a + qr_2, ..., a + qr_k$ são dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m ■

Lema 3.2.2. Sendo m e n inteiros positivos maiores do que 1 e $(m, n) = 1$, a função φ de Euler é multiplicativa, isto é, $\varphi(m.n) = \varphi(m).\varphi(n)$.

Demonstração:

Vamos considerar a tabela com o números $1, 2, 3, ..., nm$ dispostos em m linhas e n colunas.

Assim:

1	2	3	...	i	..	n
$n+1$	$n+2$	$n+3$	...	$n+i$	...	$n+n$
$2n+1$	$2n+2$	$2n+3$	...	$2n+i$	..	$2n+n$
...	...	...	...	...	...	...
$(m-1)n+1$	$(m-1)n+2$	$(m-1)n+3$	...	$(m-1)n+i$	...	$(m-1)n+n$

Pela **Proposição 2.3.1.** $(k, mn) = 1 \Leftrightarrow (k, m) = (k, n) = 1$, então para calcular $\varphi(mn)$ temos que determinar os elementos da tabela acima que são, ao mesmo tempo, primos com m e n.

Se o primeiro elemento de uma coluna não for primo com n, então todos os elementos da coluna não são primos com n. Assim os elementos primos com n estão, necessariamente nas colunas restantes que são em número $\varphi(n)$, cujos elementos são primos com n.

Agora, vejamos em cada uma dessas colunas, quais são os primos com m.

Como $(m, n) = 1$, $i, n+i, 2n+i, ..., (m-1)n+i$, pela **Proposição 3.2.2.**, formam o sistema de completo de resíduos módulo m e, portanto, $\varphi(m)$ desses elementos são primos com m.

Logo o número de elementos, simultaneamente, primos com m e n é $\varphi(m)\varphi(n)$ ■

Lema 3.2.3. Seja p um número primo e k um inteiro positivo então $\varphi(p^k) = p^k - p^{k-1}$.

Demonstração:

Usando uma contagem simples tem-se que de 1 até p^k existem exatamente p^k números inteiros positivos.

Excluiremos desses os números que não são primos com p^r, ou seja, todos os múltiplos de p. Estes são: $1p, 2p, 3p, ..., p^{n-1}p$, cujo número é p^{n-1}. Logo $\varphi(p^k) = p^k - p^{k-1}$ ■

Corolário 3.2.1. Seja p um primo, então $\varphi(p) = p - 1$.

Demonstração:

Basta tomar $k = 1$ no Lema anterior ■

Podemos agora obter uma expressão que nos dê $\varphi(n)$ para qualquer n natural.

Teorema 3.2.2. Seja n um inteiro positivo, onde $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ a decomposição primária de n, então $\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$.

Demonstração:

Considere $\varphi(n)$, onde n é um inteiro positivo, por hipótese $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, então $\varphi(n) = \varphi(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i})$, este resultado decorre do **Lema 2.4.2.**, e pelo **Lema 2.4.3.** temos que $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$, com $1 \leq i \leq k$, então $\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$ ■

Apresentaremos agora uma generalização do Pequeno teorema de Fermat realizada por Euler.

Teorema 3.2.3.(Teorema de Euler) Sejam n e m inteiros positivos, com $(n, m) = 1$. Então

$$n^{\varphi(m)} \equiv 1 \bmod m$$

Demonstração:

Seja $\{r_1, r_2, ..., r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m e $(n, m) = 1$, então pela **Proposição 3.2.1.** $\{nr_1, nr_2, ..., nr_{\varphi(m)}\}$ também será. Para cada elemento nr_i do segundo sistema, um e só um, elemento r_j do primeiro sistema é tal que $nr_i \equiv r_j \bmod m$. Então:

$$nr_1 nr_2 ... nr_{\varphi(m)} \equiv r_1 r_2 ... r_{\varphi(m)} \bmod m$$

$$n^{\varphi(m)}(r_1 r_2 ... r_{\varphi(m)}) \equiv (r_1 r_2 ... r_{\varphi(m)}) \bmod m$$

Como $(r_i, m) = 1$, temos que $(r_1 r_2 ... r_{\varphi(m)}, m) = 1$, portanto $n^{\varphi(m)} \equiv 1 \bmod m$ ■

Corolário 3.2.2. Sejam n e p inteiros tais que $(n, p) = 1$ e p primo. Então

$$n^{p-1} \equiv 1 \bmod p$$

Demonstração:

Como $\varphi(p) = p - 1$ e $n^{\varphi(p)} \equiv 1 \bmod p$ temos que $n^{p-1} \equiv 1 \bmod p$ ■

Definiremos agora um conceito importante a respeito das congruências da forma $a^n \equiv 1 \bmod m$.

Definição 3.2.4. Sejam a e m inteiros, com $m > 1$ e $(a, m) = 1$. Definiremos por *Ordem de a com relação a m*, o natural

$$ord_m(a) = min\{i \in \mathbb{N}; a^i \equiv 1 \bmod m\}$$

Cabe portanto, o seguinte lema descrito abaixo.

Lema 3.2.4. Com as condições acima definidas, $a^n \equiv 1 \bmod m$ se, e somente se, $ord_m(a)|n$.

Demonstração:

Seja $i = ord_m(a)$. Temos pelo **Teorema 2.2.1.** $n = q.i + r$, com q, r univocamente determinados e $0 \leq r < i$.

Suponhamos que $r \neq 0$, como $a^i \equiv 1 \bmod m$ temos:

$$a^{q.i} \equiv 1 \bmod m \Rightarrow a^{q.i}.a^r \equiv a^r \bmod m \Rightarrow a^n \equiv a^r \bmod m$$

Como $a^n \equiv 1 \bmod m$ temos que $a^r \equiv 1 \bmod m$ então $i < r$. Absurdo! Logo $r = 0$.

Por outro lado, se $i|n$ existe um inteiro q tal que $n = q.i$. Como $a^i \equiv 1 \bmod m$ temos:

$$a^{q.i} \equiv 1 \bmod m \Rightarrow a^n \equiv 1 \bmod m \blacksquare$$

3.3 Teorema de Wilson

Um outro critério de primalidade que também pode ser usado é o Teorema de Wilson[1], que foi provado pela primeira vez por Lagrange.

Lema 3.3.1. Sejam a e p inteiros com p primo. Se $a^2 \equiv 1 \bmod p$ então $a \equiv 1 \bmod p$ ou $a \equiv -1 \bmod p$.

Demonstração:

Sendo $a^2 \equiv 1 \bmod p$ temos que $p|a^2 - 1 = (a+1)(a-1)$, sendo p primo então tem que dividir um dos dois fatores, assim $p|(a+1)$ ou $p|(a-1)$. Portanto $a \equiv 1 \bmod p$ ou $a \equiv -1 \bmod p \blacksquare$

Teorema 3.3.1. p é um número primo se, e somente se, $(p-1)! \equiv (p-1) \bmod p$.

Demonstração:

Para $p = 2$ ou $p = 3$, o teorema verifica-se trivialmente. Suponhamos então que $p \geq 5$ é um número primo. Temos que $(p-1)! = 2.3.4...(p-2).(p-1)$, como $(p-1) \equiv (p-1) \bmod p$, para demonstrar o teorema basta mostrar que:

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

Seja $a \in \{2, 3, ...(p-2)\}$. Pelo **Teorema 2.4.1.** x é solução da congruência $ax \equiv 1 \bmod p$ se, e só se, $(a, p) = 1$ e portanto $x \in \{0, 1, 2, ...(p-1)\}$.

Note que x não pode ser igual a 0 a 1 ou a $(p-1)$, pois se $x = 0 \Rightarrow a.0 \equiv 1 \bmod p \Rightarrow p|1$, o que não ocorre.

Já se $x = 1 \Rightarrow a \equiv 1 \bmod p$ e se $x = (p-1) \Rightarrow a(p-1) \equiv 1 \bmod p$ e portanto $a \equiv -1 \bmod p$. Assim $a = 1$ ou $a = (p-1)$ o que também não ocorre, pois $a \in \{2, 3, ...(p-2)\}$. Logo $x \in \{2, 3, 4, ..., (p-2)\}$.

[1] Jhon Wilson(1741-1793), professor de matemática britânico.

Note ainda que $x \neq a$, pois se $x = a$ teríamos $a.a = a^2 \equiv 1 \mod p$, o que pelo Lema acima, implicaria $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$.

Assim para cada $a \in \{2, 3, ..., (p-2)\}$ existe $x \neq a$ no mesmo conjunto tal que $ax \equiv 1 \mod p$. E existe um só elemento nessas condições, pois se $ay \equiv 1 \mod p$ com $y \in \{2, 3, 4, ..., (p-2)\}$ teríamos:

$$ay \equiv ax \mod p \Rightarrow x \equiv y \mod p \text{ e portanto } y = x.$$

Logo $2.3...(p-2) \equiv 1 \mod p$ e como $(p-1) \equiv (p-1) \mod p$ temos:

$$2.3...(p-2)(p-1) \equiv (p-1) \mod p \Rightarrow (p-)! \equiv (p-1) \mod p.$$

Por outro lado, suponhamos que p seja composto, então existem inteiros n_1 e n_2 menores que p tais que $p = n_1 n_2$, suponhamos, sem nenhuma perda de generalidade, que $n_1 < n_2$. Então:

$$(p-1)! = 2.3.4...n_1.n_2...(p-1) \Rightarrow p|(p-1)!$$

Note que $p \nmid [(p-1)! - (p-1)]$ e portanto $(p-1)! \not\equiv (p-1) \mod p$. O que contraria a hipótese. Logo p é primo ■

Capítulo 4

Alguns Primos Especiais

Nesse capítulo apresentaremos um brevíssimo estudo sobre alguns números especiais, certas propriedades relativas a eles e os primos em uma P.A..

4.1 Primos de Mersenne

Existem algumas fórmulas que geram famílias interessantes de números primos[1], entretanto os que abordaremos aqui serão da forma $2^n - 1$.

Proposição 4.1.1. Sejam a e n inteiros maiores que 1. Se $a^n - 1$ é primo então $a = 2$ e n é primo.

Demonstração:

Suponhamos que $a \neq 2$, assim $a > 2 \Rightarrow a - 1 > 1$, pelo **Proposição 2.1.1.** $(a-1)|(a^n-1)$, então $(a^n - 1)$ seria composto, contradizendo a hipótese. Assim $a = 2$.

Suponhamos agora que n é composto, então existem n_1 e n_2 inteiros maiores que 1, tais que $n = n_1.n_2$.

Como $(a^{n_1} - 1)|(a^{n_1})^{n2} - 1^{n_2} = a^{n_1 n_2} - 1 = a^n - 1$ assim $a^n - 1$ seria composto. Absurdo!

Logo n é primo ■

Corolário 4.1.1. Se n for composto, então $2^n - 1$ também será composto.

Demonstração:

[1] Veja [11]

Seja $a = 2$ e tomemos a contra positiva da proposição anterior ■

Podemos então definir os números da forma $M_p = 2^p - 1$, com p primo, como *Números de Mersenne.* Se M_p for primo será chamado de *Primo de Mersenne.*

Desde o tempo de Mersenne era sabido que $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ são primos, enquanto que $M_{11} = 23.89$, e portanto, não é primo, isto mostra que o recíproca da proposição acima é falsa.

A fim de facilitar a busca de primos de Mersenne, podemos considerar o corolário acima, já que só será necessário comprovar a primalidade de M_n quando n for primo.

No intervalo $2 \leq p \leq 5000$, os números de Mersenne que são primos, tem para o primo p os seguintes valores:

$$2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 6071279, 2203, 2281, 3217, 4253, 4423$$

. Em 2008 foi descoberto o maior primo de Mersenne [2], este tem $p = 43112609$.

Em relação aos números de Mersenne, o problema que se apresenta naturalmente, é o de saber se são primos ou compostos e, neste ultimo caso, determinar seus divisores primos.

Através de uma trabalhosa inspeção, é possível achar os divisores de M_{11}. Assim enunciaremos abaixo uma proposição sobre os divisores dos números de Mersenne.

Proposição 4.1.2. Seja $p > 2$ um primo, então todo divisor , q primo, de M_p é da forma $k.2p + 1$, com k inteiro.

Demonstração:

Sendo q um primo, temos que $(2, q) = 1$. Seja $i = ord_q(2)$ então $2^i \equiv 1 \mod q$.

Sabemos, pelo **Corolário 3.2.2.** que $2^{q-1} \equiv 1 \mod q$, então pelo **Lema 3.2.4.** $i|(q-1)$.

Pela hipótese $q|M_p \Rightarrow 2^p \equiv 1 \mod q \Rightarrow 2^{2p} \equiv 1 \mod q$, então $i|2p$.

Suponhamos $i \neq 2p$, portanto pelo **Teorema 2.2.1.**

$$2p = t.i + r \quad , \text{com} \quad 0 < r < i$$

Como $2^i \equiv 1 \mod q \Rightarrow 2^{ti} \equiv 1 \mod q \Rightarrow 2^{ti+r} \equiv 2^r \equiv 1 \mod q$, então $i < r$. Absurdo!

Logo $i = 2p$. Assim $2p|(q-1) \Rightarrow q - 1 = k.2p \Rightarrow q = k.2p + 1$, com k inteiro. ■

[2]Descoberto por E. Smith, G.F. Woltman, S Kurowski e GIMPS foi o primeiro número primo descoberto com mais de dez milhões de algarismos, o que valeu aos descobridores o Prêmio de 100.000 dólares, outorgado pela Eletronic Frontier Fundation, para mais informação ler [11].

Considere o número de Mersenne M_{67}, sendo q um divisor primo seu, então $q = k.2.67 + 1 = 134.k + 1$, sendo $k = 1.445.580$ temos que $q = 193.707.721$ que é um divisor de M_{67} com foi mostrado em 1903 por Cole[3] no encontro da American Mathematical Society, onde ele mostrou que $M_{67} = (193.707.721)(761.838.257, 287)$ e portanto, não seria primo, além de determinar os seus fatores primos.

"Existen infinitos números de Mersenne?", esta é uma pergunta que ainda não tem resposta, há vários problemas em aberto sobre os números de Mersenne, este é um deles.

4.2 Teorema de Euclides - Euler

Trataremos nesta seção um importante teorema proposto por Euclides, nos *Elementos*, e que mais tarde, teve sua recíproca provada por Euler. Este teorema trata de uma ligação entre os números perfeitos e os números de Mersenne.

Definição 4.2.1. Chamamos de função aritmética a uma função definida para todos os inteiros positivos.A função φ de Euler descreve um exemplo de tais funções.

Definição 4.2.2. Seja a função $\sigma(n)$ definida como sendo a soma dos divisores positivos de n, ou seja

$$\sigma(n) = \sum_{d|n} d$$

Assim, temos por exemplo que $\sigma(1) = 1$, $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$ e $\sigma(p) = p + 1$ se p é primo.

Proposição 4.2.1 Seja n um inteiro, tal que $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ onde p_i é primo e α_i inteiro positivo. Então

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Demostração:

Seja d um divisor positivo de n, então $d < n$ e $d = \prod_{i=1}^{r} p_i^{\beta_i}$, com $0 \leq \beta_i \leq \alpha_i$. Com efeito, pois se $\beta_i > \alpha_i \Rightarrow p_i^{\beta_i} > p_i^{\alpha_i} \Rightarrow \prod_{i=1}^{k} p_i^{\beta_i} > \prod_{i=1}^{k} p_i^{\alpha_i} \Rightarrow d > n$ o que não ocorre.

[3]Frank Nelson Cole, 20 de setembro de 1861 - 26 de maio 1926, matemático estadunidense.

Logo a soma na definição de $\sigma(n)$ percorre todos os números da forma $d = \prod_{i=1}^{r} p_i^{\beta_i}$

Se considerarmos o fator $p_i^{\alpha_i}$ de n para algum $1 \leq i \leq k$, então os divisores desse fator são $1, p_i, p_i^2, ..., p_i^{\alpha_i}$ e portanto temos a seguinte fatoração:

$$\sigma(n) = (1 + p_1 + p_1^2 + ... + p_1^{\alpha_1}).(1 + p_2 + p_2^2 + ... + p_2^{\alpha_2})...(1 + p_k + p_k^2 + ... + p_k^{\alpha_k})$$

Note que cada um dos fatores desse produto escreve a soma dos termos de *Progressão Geométrica*[4]. Então para cada fator teremos:

$$1 + p_i + p_i^2 + ... + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Então $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$. ■

Corolário 4.2.1. Se $(m, n) = 1$ então $\sigma(n.m) = \sigma(n).\sigma(m)$.

Demonstração:

Sejam $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ e $m = \prod_{i=1}^{r} q_i^{\beta_i}$, com $p_i \neq q_i$, pois $(n, m) = 1$, então $m.n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}.q_1^{\beta_1}.q_2^{\beta_2}...q_r^{\beta_r}$.

Assim $\sigma(m.n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}.\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1}...\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.\frac{q_1^{\beta_1+1} - 1}{q_1 - 1}.\frac{q_2^{\beta_2+1} - 1}{q_2 - 1}...\frac{q_r^{\beta_r+1} - 1}{q_r - 1} = \sigma(m).\sigma(n)$. ■

Proposição 4.2.2. Seja n um inteiro positivo, $\sigma(n) = n + 1$ se, e somente se, n é um número primo.

Demonstração:

Se $\sigma(n) = n + 1$, $n > 1$ e os únicos divisores de n são 1 e n, logo n é primo.

Por outro lado, se n é um número primo, seus únicos são n e 1, então a soma dos divisores de n será $n + 1$. Logo $\sigma(n) = n + 1$. ■

Definição 4.2.3. Seja n um número inteiro positivo, dizemos que n é um *Número Perfeito* se ele for igual a soma de seus divisores positivos menores que n.

[4]Ver Apêndice

Utilizando-se da função $\sigma(n)$, um número é perfeito se $\sigma(n) = 2n$, por exemplo $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2.6$, ou seja, 6 é um número perfeito.

Os números perfeitos já eram conhecidos desde a antiguidade. O menor número perfeito, 6, era ligado pelos escribas, místicos e religiosos, à perfeição; isso justificava a criação do mundo ter sido realizada em 6 dias. São também números perfeitos os números: $28, 496, 8128$ e 33550336.

Atualmente, conhecem-se mais alguns números perfeitos. Um fato curioso é que todos os números perfeitos conhecidos são pares. Não se sabe se existem, ou não, números perfeitos ímpares.

Enunciaremos agora o Teorema de Euclides-Euler.

Teorema 4.2.1. Seja n um inteiro positivo e M_p um primo de Mersenne, n é um número perfeito par se, e somente se, $n = 2^{p-1}.M_p$.

Demonstração:

Sendo n um número par, tomemos 2^{r-1} a maior potência de 2 que divide n, então: $n = 2^{r-1}.k$, com k inteiro, então $r > 1$ e k é ímpar, portanto $(2^{r-1}, k) = 1$. Assim:

$$\sigma(n) = \sigma(2^{r-1}.k) = \sigma(2^{r-1}).\sigma(k) \Rightarrow 2n = \sigma(2^{r-1}).\sigma(k) \Rightarrow 2.2^{r-1}.k = \frac{2^{r-1+1} - 1}{2 - 1}\sigma(k).$$

Portanto:

$$2^r.k = (2^r - 1)\sigma(k) \tag{4.1}$$

Note que, $(2^r, 2^r - 1) = 1$, de 4.1 e sendo a um inteiro positivo, terremos:

$$k = a(2^r - 1) \tag{4.2}$$

De 4.1 e 4.2, teremos:

$$2^r.a(2^r - 1) = (2^r - 1).\sigma(k)$$

Logo:

$$\sigma(k) = 2^r.a \tag{4.3}$$

De 4.2 e 4.3, temos que $k = a.2^r - a \Rightarrow a2^r = k + a \Rightarrow \sigma(k) = k + a$. Nesta situação $a = 1$. De fato, pois se $a \neq 1$, de 4.2, a seria um divisor de k, então $\sigma(k) \geq 1 + a + k > a + k = \sigma(k)$. Absurdo!

Logo $k = (2^r - 1) = M_r$.

Portanto $\sigma(k) = k + 1$, pela **Proposição 4.2.2.** k é primo. Segue-se que $n = 2^{r-1}.M_r$.

Por outro lado, se $n = 2^{r-1}.M_r$ então $r > 1$, e, consequentemente, n é par.

Note que $(2^{p-1}, 2^p - 1) = 1$, pois $2^p - 1$ é ímpar, e pelo **Corolário 4.2.1.**, segue-se que

$$\sigma(n) = \sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{2^{p-1+1} - 1}{2 - 1}.(2^p - 1 + 1) = (2^p - 1).2^p = 2n. \blacksquare$$

4.3 Números de Fermat

Muitos números com formato particular são largamente estudados em Teoria dos Números. Para estes números existem métodos mais específicos para testar se eles são primos ou compostos.

Desde de muito tempo, tem havido um interesse grande pelos números da forma $2^m + 1$, o estudo dos números de Mersenne é um exemplo.

Como foi falado no Capítulo 2, os números dessa forma, onde $m = 2^n$, ou seja, $F_n = 2^{2^n} + 1$ é chamado de Número de Fermat.

Fermat conjecturou que todos os números dessa forma seriam primos, mais Euler provou que $F_5 = 2^{2^5} + 1$ não seria.

Na proposição abaixo mostraremos que os divisores primos de F_n aparecem sob uma forma específica.

Proposição 4.3.1. Seja F_n um número de Fermat, então todo divisor p primo de F_n é da forma $k.2^{n+1} + 1$.

Demonstração:

Seja $i = ord_p(2)$, assim $2^i \equiv 1 \bmod p$, e se p é um primo tal que $p|F_n = 2^{2^n} + 1$, então p é ímpar, já que F_n é ímpar.

Note que $i \nmid 2^n$, pois, caso contrário, pelo **Lema 3.2.4.** $2^{2^n} \equiv 1 \bmod p \Rightarrow 2^{2^n} + 1 \equiv 2 \bmod p \Rightarrow 2 \equiv 0 \bmod p$, o que é falso, pois p é ímpar.

Assim:

$$2^{2^n} \equiv -1 \bmod p \Rightarrow (2^{2^n})^2 \equiv (-1)^2 \bmod p \Rightarrow 2^{2^{n+1}} \equiv 1 \bmod p$$

Ainda pelo **Lema 3.2.4.** $i|2^{n+1}$ e como $i \nmid 2^n$, segue-se que $i = 2^{n+1}$. Como $(2, p) = 1$ e pelo **Corolário 3.2.2.**

$$2^{p-1} \equiv 1 \bmod p \Rightarrow i|(p-1).$$

Então existe k inteiro tal que:

$$(p-1) = k.2^{n+1} \Rightarrow p = k.2^{n+1} + 1.$$

Portanto todo divisor de F_n é da forma $k.2^{n+1} + 1$.■

Portanto todos os divisores primos dos números de Fermat são da forma $k.2^{n+1} + 1$. Assim um divisor primo de F_5 será da forma $k.2^6 + 1$, com k um inteiro positivo.

Fazendo k variar de 1 a 10, encontraremos os números:

$$65, 129, 193, 257, 321, 385, 449, 513, 577 \text{ e } 641,$$

dos quais apenas $193, 257, 449, 577, 641$ são primos. Agora precisamos testar, um a um, estes valores, começaremos pelo o maior deles, e veremos que:

$2^{16} = 65\ 536 \equiv 154 \bmod 641$, então $(2^{16})^2 \equiv (154)^2 = 23\ 716 \equiv 640 \bmod 641$.

Portanto:

$$2^{32} \equiv 640 \bmod 641 \Rightarrow 2^{32} + 1 \equiv 641 \equiv 0 \bmod 641.$$

Assim $641|(2^{32} + 1) = (2^{2^5} + 1) = F_5$ e que portanto não seria primo.

Como este resultado já era conhecido, tornou-se conveniente tomarmos o primo 641 para testarmos a primalidade de F_5, entretanto, é possível, porém bastante trabalhoso, testarmos todos os outros valores e verificar a afirmação dada por Euler.

O maior número primo de Fermat conhecido é $F_4 = 65637$ e o maior número de Fermat composto conhecido é $F_{2478782}$, com o fator $3.2^{2478785} + 1$ que tem 746190 algarismos.

Mostraremos adiante um teste de primalidade para os números de Fermat. Para tanto, necessitamos de alguns resultados derivados da *Teoria dos Resíduos Quadráticos*[5], estes resultados exibiremos sem prova, pois direcionamos nossa atenção para testar a primalidade de um número de Fermat.

Seja a congruência $x^2 \equiv a \bmod m$, com a e m inteiros e $m > 1$. Quando esta congruência possui alguma solução, diz-se que a é *resíduo quadrático módulo* m. Por

[5] A formalização dos resultados encontram-se em [6].

exemplo a congruência $x^2 \equiv 2 \bmod 3$, nãopossui nenhuma solução.

Se p é um número primo ímpar, define-se o *Símbolo de Legendre*, como sendo

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

Proposição 4.3.2. Sejam a, b inteiros e p um primo, tal que $(a,p) = (b,p) = 1$.

1. Se $a \equiv b \bmod p$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$.

Teorema 4.3.1.(Lei da Reciprocidade Quadrática) Sejam p e q primos ímpares distintos. Então

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

Proposição 4.3.3. Seja $n > 1$. Se para cada fator primo q de $n-1$, existe um inteiro a, tal que $a^{n-1} \equiv 1 \bmod n$ e $a^{\frac{n-1}{q}} \not\equiv \bmod n$, então n é primo.

Demonstrção:

Seja q um primo e $r > 1$ um inteiro, tal que q^r é a maior potência de q que divide $n-1$.

Seja $i = ord_n(a)$, como $a^{n-1} \equiv 1 \bmod n$ e $a^{\frac{n-1}{q}} \not\equiv \bmod n$. Temos que $i|(n-1)$ e $i \nmid \frac{(n-1)}{q}$ e, consequentemente, $q^r|i$. Como $a^{\varphi(n)} \equiv 1 \bmod n$, então

$$i|\varphi(n) \Rightarrow q^r|\varphi(n).$$

Logo $(n-1)|\varphi(n)$ e sendo $\varphi(n) \leq n-1$ temos que $n-1 = \varphi(n)$. Portanto n é primo. ■

Voltaremos agora nossa atenção a primalidade dos números de Fermat.

Proposição 4.3.4. (Teste de Pepin[6]) Seja $F_n = 2^{2^n} + 1$, com n inteiro maior que 1. F_n é primo se, e somente se, $3^{\frac{F_n-1}{2}} \equiv -1 \bmod F_n$.

[6]Jean François Théophile Pépin Cluses, 14 maio 1826 - Lione, 3 abril de 1904, matemático francês

Demonstração:

Seja F_n um primo de Fermat, então pela Lei da Reciprocidade Quadrática

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{F_n-1}{2}} = \left(\frac{F_n}{3}\right)(-1)^{(F_n-1)/2} = \left(\frac{F_n}{3}\right)$$

já que $\dfrac{F_n-1}{2}$ é par.

Note que:

$2^2 \equiv 1 \bmod 3 \Rightarrow 2^{2^n} \equiv 1 \bmod 3 \Rightarrow 2^{2^n}+1 \equiv 2 \bmod 3$ então $F_n \equiv 2 \bmod 3$.

Tomando o item (1). da **Proposição 4.3.2.** $\left(\dfrac{F_n}{3}\right) = \left(\dfrac{2}{3}\right) \Rightarrow \left(\dfrac{3}{F_n}\right) = \left(\dfrac{2}{3}\right)$, como 2 não é resíduo quadrático módulo 3, temos que $\left(\dfrac{3}{F_n}\right) = -1$. Usando o item (2). da mesma proposição, $3^{\frac{F_n-1}{2}} \equiv \left(\dfrac{3}{F_n}\right) = -1 \bmod F_n$.

Por outo lado, se $3^{\frac{F_n-1}{2}} \equiv 1 \bmod F_n \Rightarrow 3^{F_n-1} \equiv 1 \bmod F_n$ a primalidade de F_n obtém-se pela **Proposição 4.3.3.** .■

Como exemplo do teste acima, mostraremos que F_4 é primo.

Para que o teste funcione devemos mostrar que:

$$3^{(F_4-1)/2} \equiv -1 \bmod F_4$$

.

Como $F_4 = 65537$, temos que $\dfrac{F_4-1}{2} = \dfrac{65536}{2} = 32768 = 2^{15}$. Como $2^{2^{15}} \equiv -1 \bmod (65537)$, F_4 é primo.

4.4 Primos em Progressão Aritmética

Observando a sequência numérica abaixo:

$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, ...$

vemos que nela aparecem vários números primos, além de que ela expressa os números da forma $4n+3$, com n sendo inteiro positivo.

Naturalmente poderíamos perguntar se são escritos infinitos números primos nesta sequência. A resposta é sim, e podemos provar tal fato. Para tanto, utilizaremos o mesmo método que Euclides usou nos *Elementos* para demonstrar a existência de infinitos números primos.

Suponhamos que existisse um número finito de primos da forma $4n+3$, vamos denominá-los $q_1, q_2, q_3, ..., q_n$. Sendo N um número inteiro positivo, Pelo **Teorema 2.2.1.**, $N = 4n + r$, com $0 \leq r \leq 3$, portanto todo número ímpar é da forma $4n+3$ ou $4n+1$.

Note que, o produto de dois números da forma $4n+1$ será também da forma $4n+1$. Com efeito, pois sendo r, s e k inteiros positivos e, considerando os ímpares $4r+1$ e $4s+1$, temos:

$$(4r+1).(4s+1) = 4(4rs + r + s) + 1 = 4k + 1$$

Sendo o número $N = 4(q_1q_2q_3...q_n) + 3$ temos que N não é divisível por nenhum dos números primos $3, q_1, q_2, q_3, ..., q_n$, portanto na decomposição de N, em fatores primos, só podem aparecer primos da forma $4n+1$, logo N é da forma $4n+1$. Absurdo! Sendo assim, concluímos que existe um número infinito de primos da forma 4n + 3.

A pergunta seguinte seria:"Existe um número infinito de primos da forma $4n+1$?"A resposta a esta pergunta também será afirmativa, porém devemos utilizar um outro argumento bem mais elaborado para resolver esta questão.

Uma situação semelhante surge em relação às sequências de números da forma $6n+1$ e $6n+5$. Observe que às sequências da forma $4n+1$, $6n+1$ ou $6n+5$, tratam-se de Progressões Aritméticas$(P.A.)$[7].

$4n+1$, $4n+3$, $2n+5$, $10n+3$ são também exemplos de Progressões Aritméticas. Esta observação nos leva a uma pergunta:

"Será que o fato de existirem infinitos primos em algumas progressões aritméticas, pode ser generalizado?"

As $P.A.'s$ citadas acima são da forma $a+nq$ onde a, b e n são inteiros, a e q são fixados e $n \geq 0$ ou seja

$$a, a+q, a+2q, a+3q, a+4q, ...$$

[7]É toda sequência $(a_n)_{n\in\mathbb{N}}$ definida da seguinte forma: $a_1 = a$; $a_n = a_{n-1} + q$, com a e q números reais dados.

Note que $(a, q) = 1$, pois se a e q possuem um fator comum, isto é, se $(a, q) \neq 1$, $(a, q)|(a + nq)$ e tal progressão aritmética não conteria números primos, pois todo elemento da progressão teria esse fator. Por exemplo, consideremos a progressão aritmética dada por $4+2n$, vemos que $(a, q) = (4, 2) = 2$ então todos os seus termos são pares e portanto não aparecem números primos na sequencia.

Esse fato nos leva a considerar apenas $P.A.'s$ da da forma $a + nq$ em que a e q sejam primos entre si, para que possamos obter um número infinito de primos nesta sequencia.

Muitos casos particulares nos são conhecidos, como o caso em que $a = 1$ e $q = 2$, ou seja a progressão aritmética $1 + 2n$, que descreve todos os números ímpares, e pelo **Teorema (2.5.1.)**, temos que nessa $P.A.'s$ existem infinitos números primos. Provaremos agora um caso mais geral em que $q = 4, 8, 16, 32, ...$ ou seja $q = 2^r$ e $a = 1$.

Proposição 4.4.1. Na progressão aritmética de primeiro 1 e razão 2^r, para r natural fixo, existem infinitos números primos.

Demonstração:

Pelo **Lema 2.3.3.** $(F_n, F_m) = 1$, se $n \neq m$ então os divisores de F_n são dois a dois disjuntos, e como esses divisores de são da forma $k.2^{n+1} + 1$, sendo $r = n + 1$, temos que na sequência $1 + k.2^r$, com $k \geq 0$ inteiro, existem infinitos primos. ■

Enunciamos o seguinte teorema, que foi conjecturado por Legendre, mas foi de fato demonstrado por Dirichlet, em 1837.

Teorema 4.4.1. Se $q \geq 2$ e $a \neq 0$ são inteiros primos entre si, então a progressão aritmética

$$a, a + q, a + 2q, a + 3q, ...$$

contém uma infinidade de números primos.

Trataremos aqui apenas a demonstração dada por Euler, para o caso em que $q = 2$, já que o escopo deste trabalho não nos permitirá realizar tal façanha, pois a demonstração deste fortíssimo teorema recorre a ferramentas avançadas e engenhosas pertencentes a Teoria Analítica dos Números[8].

Antes de realizarmos tal demonstração, introduziremos mais alguns conceitos matemáticos e chegaremos a uma importante igualdade chamada de *Produto de Euler*.

[8] Trata-se do ramo da Matemática, em particular da Teoria dos Números, que usa métodos de análise matemática para demonstrar seus resultados.

Durante boa parte da sua vida, Euler dedicou-se ao estudo das séries infinitas[9]. Em matemática, o conceito de série surge de maneira a tentar generalizar a soma para uma infinidade de parcelas. Em meio a tantos exemplos, uma delas, a série $\sum_{n=1}^{\infty} \frac{1}{n^s}$, que se prova ser convergente sempre que $S > 1$ tem especial importância no estudo da teoria dos números.

Proposição 4.4.2. Seja $s > 1$, então a série $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converge.

Demonstração:

Seja $f(x) = \frac{1}{x^s}$, do cálculo, sabemos que f é contínua, positiva e decrescente no intervalo real $(1, \infty)$, aplicando o Teste da Integral[10], temos:

$$\int_1^{\infty} \frac{1}{x^s} dx = \lim_{t\to\infty} \int_1^t \frac{1}{x^s} dx = \lim_{t\to\infty} \left(\frac{t^{-s+1}}{-s+1} - \frac{1}{-s+1} \right) = \frac{1}{-s+1} \lim_{t\to\infty} \left(\frac{1}{t^{s-1}} - 1 \right).$$

Como $s > 1 \Rightarrow s - 1 > 0 \Rightarrow \frac{1}{t^{s-1}} \to 0$ quando $t \to \infty$.Portanto $\int_1^{\infty} \frac{1}{x^s} = \frac{1}{s-1}$, quando $s > 1$.

Assim, a integral converge, e portanto, pelo teste da integral, a série converge. ■

Definição 4.4.1. Seja $s > 1$ definiremos a função Zeta(ζ), como

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

O teorema seguinte mostra-nos que existe uma forte relação entre a função ζ e os números primos. Para tanto provemos o teorema abaixo.

TEOREMA 4.4.1.(Produto de Euler) Se $s > 1$ então

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\ primo} \frac{1}{1 - \frac{1}{p^s}}$$

.

[9]Ver Apêndice A
[10]Ver Apêndice A

Demonstração:

Seja x um número real tal que $|x| < 1$. Temos que $\sum_{i=1}^{\infty} x^i = \frac{1}{1-x}$ pois trata-se da soma de uma Progressão Geométrica Infinita.

Sendo p um primo e $s > 1$, temos que $\left|\frac{1}{p^s}\right| < 1$, portanto

$$\sum_{i=1}^{\infty} \frac{1}{p^{si}} = \frac{1}{1-\frac{1}{p^s}}.$$

Multiplicando a igualdade acima por todos os primos p teremos:

$$\prod_{p\ primo} \frac{1}{1-\frac{1}{p^s}} = \prod_{p\ primo} \sum_{i=1}^{\infty} \frac{1}{p^{si}}.$$

Desenvolvendo o segundo membro desta equação teremos:

$$\prod_{p\ primo} \sum_{i=1}^{\infty} \frac{1}{p^{si}} = \left(1+\frac{1}{2^s}+\frac{1}{2^{2s}}+...\right)\left(1+\frac{1}{3^s}+\frac{1}{3^{2s}}+...\right)\left(1+\frac{1}{5^s}+\frac{1}{5^{2s}}+...\right)...$$

Portanto:

$$\prod_{p\ primo} \sum_{i=1}^{\infty} \frac{1}{p^{si}} = 1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{5^s}+...+\frac{1}{(2.3.5...)^s}+...$$

Pelo **Teorema 2.3.1.** cada denominador escreve um número inteiro positivo distinto, então:

$$\prod_{p\ primo} \sum_{i=1}^{\infty} \frac{1}{p^{si}} = 1+\frac{1}{2^s}+\frac{1}{3^s}+...+\frac{1}{n^s}+...$$

Logo: $\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\ primo} \frac{1}{1-\frac{1}{p^s}}$. ■

Embora já tenhamos provado esse resultado, daremos uma outra demonstração para a existência de infinitos primos, abordando a progressão aritmética de primeiro termo 1 e razão 2. Esta demonstração foi dada por Euler e aborda o uso da relação por ele descoberta, o Produto de Euler. Assim, vamos a seguinte proposição.

Proposição 4.4.3. Seja $n \geq 0$ um inteiro, então existem infinitos primos na sequência $1 + 2n$.

Demonstração:

Primeiro lembremo-nos da *expansão em séries de potências*[11] para o $\ln(1+x)$. Temos que

$$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^n}{n+1} x^{n+1}, com \quad |x| < 1. \tag{4.4}$$

Pelo teorema anterior $\zeta(s) = \prod_{p\ primo} (1-p^{-s})^{-1}$ e tomando o logaritmo natural nos dois membros dessa igualdade:

$$\ln \zeta(s) = \ln \left[\prod_{p\ primo} (1-p^{-s})^{-1} \right] = -1.\ln \prod_{p\ primo} (1-p^{-s})^{-1} = -1. \sum_{p\ primo} \ln(1-p^{-s}).$$

De 4.4, $\ln(1+(-p^{-s})) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k}(-p^{-s})^k = \sum_{k=1}^{\infty} \frac{(-1)^{k-1-k}}{k}(p^{-sk}) = -1. \sum_{k=1}^{\infty} \frac{p^{-sk}}{k}$

Logo

$$\ln \zeta(s) = \sum_{p\ primo} \sum_{k=1}^{\infty} \frac{p^{-sk}}{k}$$

.

Podemos escrever $\ln \zeta(s)$ da seguinte maneira:

$$\ln \zeta(s) = \sum_{p\ primo} \left(\frac{p^{-s}}{1} + \sum_{k=2}^{\infty} \frac{p^{-sk}}{k} \right) = \sum_{p\ primo} \frac{1}{p^s} + \sum_{p\ primo} \sum_{k=2}^{\infty} \frac{p^{-sk}}{k}.$$

Agora seja $\psi(s) = \sum_{p\ primo} \sum_{k=2}^{\infty} \frac{p^{-sk}}{k}$, temos que:

$$\psi(s) < \sum_{p\ primo} \sum_{k=2}^{\infty} p^{-sk} = \sum_{p\ primo} \left(\frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \frac{1}{p^{4s}} + ... \right) = \sum_{p\ primo} \frac{1/p^{2s}}{1 - \frac{1}{p^s}} = \sum_{p\ primo} \frac{1}{p^{2s} - p^s} <$$

[11] Ver Apêndice A

$$\sum_{p\ primo} \frac{1}{p^2} < \sum_{n=1}^{\infty} \frac{1}{n^2} = \zeta(2).$$

Então $\psi(s) < \zeta(2)$ e $\ln \zeta(s) - \zeta(2) < \sum_{p\ primo} \frac{1}{p^s}$.

Note que $\ln \zeta(s) \longrightarrow \infty$ desde que $s \longrightarrow 1^+$ e como $\psi(s)$ é limitada, concluímos que a série $\sum_{p\ primo} \frac{1}{p}$ diverge.

Este fato implica claramente a infinitude de números primos na sequência $1+2n$

■

Apêndice A

Apêndice

Trazemos aqui alguns resultados de complementação do texto, que não serão tratados profundamente, pois os conhecemos do estudo das sequências (P.A. e P.G.) e do Cálculo (Estudo das Séries).

A.1 Progressões

1. **Progressão Aritmética**

Chama-se de *Progressão Aritmética* (P.A.) uma sequência definida pela seguinte fórmula de recorrência:

$$\begin{cases} a_1 = a \\ a_n = a_{n-1} + r \quad \text{para todo } n \text{ inteiro maior ou igual que } 2 \end{cases}$$

onde a e r são números reais dados. Assim uma P.A. é uma sequência em que cada termo, a partir do segundo, é a soma do anterior com uma constante r dada.

Eis alguns exemplos:

1. $(1, 3, 5, 7, 9, ...)$ em que $a_1 = 1$ e $r = 2$
2. $(4, 4, 4, 4, 4, ...)$ em que $a_1 = 4$ e $r = 0$

Utilizando a recorrência definida acima chegamos a expressão $a_n = a_1 + (n-1)r$, chamada Termo Geral de uma P.A.. São exemplos de Termos Gerais de P.A.'s:

1. $a_n = 1 + 2(n-1)$, que escreve todos os números ímpares
2. $a_n = 6 + 5(n-1)$ que representa os inteiros $6, 11, 16, 21, 26, 31, ...$

2. Progressão Geométrica

Chamamos de *Progressão Geométrica* (P.G.) uma sequência definida pela recorrência

$$\begin{cases} a_1 = a \\ a_n = a_{n-1}.q \quad \text{para todo } n \text{ inteiro maior ou igual que } 2 \end{cases}$$

onde a e q são reais dados.

Podemos definir portanto, uma P.G. como sendo uma sequência em que cada termo, a partir do segundo, é o produto do anterior por uma constante.

São exemplos de P.G.

1. $1, 2, 4, 8, 16, ...$ onde $a_1 = 1$ e $q = 2$
2. $5, -5, 5, -5, ...$ onde $a_1 = 5$ e $q = -1$

Assim como nas P.A.'s exibiremos, a partir da recorrência acima, uma expressão que descreve todos os termos de uma P.G.. Assim o Termo Geral de uma P.G. é dado por $a_n = a_1.q^{n-1}$.

É de nosso interesse também observamos que dada uma P.G., finita, de termos $(a_1, a_2, a_3, ..., a_n)$ é possível estabelecer uma expressão que determine a soma destes termos.

Portanto a soma dos n termos de uma P.G. é:

$$S_n = \frac{a_1(q^{n-1} - 1)}{q - 1}$$

Podemos considerar Progressões Geométricas com infinitos termos, e sob certas condições, determinar o limite de sua soma. Para tanto é importante notar que toda sequência da forma $a_n = q^n$, com $-1 < q < 1$, converge para zero, isto é,

$$\text{Se } |q| < 1, \text{ então } \lim_{n \to +\infty} q^n = 0.$$

Diante disso, se q é a razão da P.G. $(a_1, a_2, a_3...)$ e $|q| < 1$, então sendo $S = \lim_{n \to +\infty} S_n$ temos que $S = \frac{a_1}{1 - q}$, onde S_n é a soma dos termos da P.G.

Um interessante resultado da aplicação do limite acima é obtido na sequência $(1, x, x^2, x^3, x^4, ...)$ é

$$1 + x + x^2 + x^3 + ... = \frac{1}{1 - x}, \text{ com } |x| < 1.$$

A.2 Séries Infinitas

1. **Série Infinita**

Um série infinita é uma expressão da forma

$$\sum_{n=1}^{\infty} a_n = a_1 + a_2 + a_3 + ... + a_n + ...$$

São muitas, além de importantíssimas, as séries infinitas em matemática, por exemplo, a série $\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + ...$ chamada de *Série Harmônica* ou $\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + ...$ a *série dos inversos dos quadrados.*

Sendo $S_n = a_1 + a_2 + ... + a_n$, se e existir o limite

$$S = \lim_{n \to \infty} S_n$$

diremos que a série $\sum_{n=1}^{\infty} a_n$ é *convergente* e S será chamado a *soma* da série, e escrevemos $S = \sum_{n=1}^{\infty} a_n$. Se uma série não converge então esta *diverge.*

Um dos problemas centrais no estudo das séries consiste em saber se uma dada série converge ou não. Há vários critérios para testar a convergência de uma série.

Destacaremos o *Teste da Integral*, pois no Capítulo 2, lançamos mão dele no estudo da série $\sum_{n=1}^{\infty} \frac{1}{n^s}$, com $s > 1$.

2. **Teste da Integral**

Se $f(x)$ é uma função positiva não crescente para $x > 0$, então a série $\sum_{n=1}^{\infty} f(n)$ converge se, e somente se, a integral imprópria $\int_1^{\infty} f(x)dx$ converge.

Exemplificaremos a aplicação do Teste acima verificando se a série $\sum_{n=2}^{\infty} \frac{1}{n \ln n}$ converge ou não.

Sendo

$$f(x) = \frac{1}{x \ln x}$$

vemos que se $x > 0$ $f(x)$ é positiva e decrescente, satisfazendo a hipótese do Teste.

Então:

$$\int_2^t \frac{1}{x \ln x} dx = \int_{\ln 2}^{\ln t} \frac{1}{u} du = \ln(\ln t) - \ln(\ln 2)$$

Este resultado obtém-se realizando a substituição $u = \ln x$. Note que

$$(\ln(\ln t) - \ln(\ln 2)) \to \infty$$

quando $t \to \infty$. Portanto a integral diverge.

Podemos concluir então que a série $\sum_{n=2}^{\infty} \frac{1}{n \ln n}$ diverge.

A.3 Serie de Potências

1. **Série de Potências**

Uma série de potência é uma série da forma

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + 1x + a_2 x^2 + ...$$

onde x é uma variável e c_n's são chamados coeficientes da série.
Em geral, a série da forma

$$\sum_{n=0}^{\infty} a_n (x-a)^n = a_0 + a_1(x-1) + a_2(x-2)^2 + ...$$

é denominada série de potências em $(x-a)$

Teorema 1: Para uma série de potências $\sum_{n=0}^{\infty} a_n (x-a)^n$ existem apenas três possibilidades:

1. A série converge apenas quando $x = a$;
2. A série converge para todo x;

3. Existe um número positivo R tal que a série converge se $|x-a| < R$ e diverge se $|x-a| > R$.

O número R no item (3). é chamado de raio de convergência da série de potências.

1. **Integração de Série de Potências**

Se a série de potências $\sum_{n=0}^{\infty} a_n(x-a)^n$ tiver um raio de convergência $R > 0$, então a função f definida por:

$$f(x) = \sum_{n=0}^{\infty} a_n(x-a)^n$$

é diferenciável (e portanto contínua) no intercalo $(a-R, a+R)$ e

$$\int f(x)dx = C + \sum_{n=0}^{\infty} a_n \frac{(x-a)^{n+1}}{n+1}.$$

Escreveremos a série de potências para a função $f(x) = \ln(1-x)$.

Notemos que, exceto por um fator de -1 a derivada dessa função é $\frac{1}{1-x}$.

Considerando a expressão $\frac{1}{1-x} = 1 + x^2 + x^3 + ...$, com $|x| < 1$ e integramos ambos os lados.

$$\int \frac{1}{1-x}dx = \int (1 + x + x^2 + x^3 + ...)dx.$$

Portanto

$$-\ln(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + ... + C$$

Para determinarmos o valor da constante C, colocamos $x = 0$ e obtemos $-\ln(1-0) = C$. Então $C = 0$.

Logo

$$-\ln(1-x) = \sum_{n=0}^{\infty} \frac{x^{n+1}}{n+1}.$$

Portanto podemos escrever a expressão em série de potências para $\ln(1+x)$ como

$$\ln(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^n}{n+1} x^{n+1}.$$

Referências Bibliográficas

[1] Ávila, G. S. S., *Cálculo Diferencial e Integral*,vol 2.2a ed.Rio de Janeiro:LTC,(1978).

[2] Boyer, C. B.,*História da Matemática*.2a ed.São Paulo:Edgard Blücher,(1996).

[3] Domingues, H.,Iezzi, G..*Álgebra Moderna*.4a ed.Sã Paulo:Atual,(2003).

[4] Domingues, H.,*Fundamentos de Aritmética*.3a ed.São Paulo:Atual,(1991).

[5] Hefez, A.,*Curso de Álgebra*,vol 1.3a ed.Rio de Janeiro:IMPA,(2002).

[6] Hefez, A., *Elementos de Aritmética*, Textos Universitários.2a ed.Rio de Janeiro:SBM,(2011).

[7] Iezzi, G.,Hazzan, S.,*Fundamentos de Matemática Elementar*,vol 4,7a ed.São Paulo:Atual,(2004).

[8] Lima, E. L.,*Curso de Análise*,vol 1.Projeto Euclides.13a ed.Rio de Jneiro:IMPA,(2011).

[9] Martines,F. B.;et al, *Teoria dos Números:Um passeio com primos e outros números familiares pelo mundo inteiro*.2a ed.Rio de Janeiro:IMPA,(2011)

[10] Muniz Neto, A. C.,*Tópicos de Matemática Elementar: Teoria dos Números*,vol 5.1a ed.Rio de Janeiro:SBM,(2012).

[11] Ribenboim,P., *Números Primos. Velhos Mistérios e Novos Recordes*,Coleção Matemática Universitária,1ed,Rio de Janeiro:IMPA, (2012).

[12] Santos, J. P. O., *Introdução à Teoria dos Números*,Coleção Matemática Universitária.3a ed.Rio de Janeiro:IMPA,(2010).

[13] Stewart J., *Cálculo*,vol 2.São Paulo:Thomson Learning,(2007).