UNIVERSIDADE TIRADENTES

EDLAMARY NUNES DE ANDRADE

VANESSA DA HORA SANTOS

“A MATEMATICA DOS NÚMEROS PRIMOS”.

Propriá
2009

EDLAMARY NUNES DE ANDRADE
VANESSA DA HORA SANTOS

“A MATEMATICA DOS NÚMEROS PRIMOS”.

Monografia apresentada a Universidade Tiradentes como um dos pré-requisitos para a obtenção do grau de Licenciatura em Matemática.

ORIENTADOR:
ANTONIO JOSÉ DE JESUS SANTOS

Propriá
2009

EDLAMARY NUNES DE ANDRADE
VANESSA DA HORA SANTOS

“A MATEMATICA DOS NÚMEROS PRIMOS”.

Monografia apresentada ao curso de Matemática da Universidade Tiradentes – UNIT, como requisito parcial para obtenção do grau de Licenciatura em Matemática.

Aprovado em _____/_____/_____.

Banca examinadora

_____

Orientador

Universidade Tiradentes

_____

Nome do professor

Universidade Tiradentes

_____

Nome do Professor

Universidade Tiradentes

DEDICATÓRIA

Dedicamos o fruto desta etapa acadêmica aos inúmeros indivíduos colaboradores da constante superação em todos os momentos de nossas vidas. Especialmente a quem nos deu a vida e razões para viver Deus.

AGRADECIMENTOS

Agradecemos ao pai pela tua proteção no dia de ontem e no dia de hoje. Os trabalhos aos quais me dediquei foram profícuos, graças á tua proteção e eu como uma criatura agradecida, venho aos teus pés exultante, dar oferenda em sentimentos das minhas vitorias, pois sei que tudo na vida esta em tuas mãos santas.

Agradecemos ao s familiares pelas palavras consoladoras que me chegaram de todas as formas e aos amigos que tiveram sua contribuição. Ao Antonio José De Jesus Santos nossos honrosos agradecimentos.

EPÍGRAFE

"A Evolução é a Lei da Vida, o Número é a Lei do Universo,a Unidade é a Lei de Deus."

Pitágoras

RESUMO

Externaremos neste trabalho em forma de análise e conhecimento no campo da Matemática, a história da matemática dos números primos, pois são conhecidos pela humanidade há muito tempo. No papiro Rhindi, por exemplo, há indícios de que o antigo povo egípcio já possuía algum conhecimento sobre esse tipo de números. No entanto, os registros mais antigos de um estudo explícito sobre números primos é devido aos gregos e a atribuição da escola de Pitágoras. Os Elementos de Euclides (cerca de 300 aC), contém teoremas importantes sobre números primos, incluindo a demonstração de sua infinitude o teorema fundamental da aritmética. Euclides também mostrou como construir um número perfeito a partir de um primo de Mersenne. Esta questão também foi resolvida na Antiguidade por Eratóstenes (276-194 a. C.), a primeira pessoa, até onde se sabe que produziu tabelas de números primos. Sendo o conceito dos números primos um fator muito importante na teoria dos números, os tipos, seus teoremas, conjeturas, hipóteses, tamanhos, aplicações e algumas demonstrações. Ao grego Eratóstenes, atribui-se um método simples para o cálculo de números primos, conhecido atualmente como crivo de Eratóstenes. Por outro lado, nos tempos atuais, os grandes números primos são encontrados com base dos códigos de segurança de informação para computadores, através de testes de primalidade mais sofisticados, como por exemplo, o teste de primalidade AKS.

PALAVRAS-CHAVE: Matemática, Números Primos Conhecidos.

ABSTRACT

External action in this work in the form of analysis and knowledge in the field of mathematics, the history of mathematics of prime numbers, as they are known to humanity for a long time. In the Rhind papyrus, for example, there is evidence that the ancient Egyptian people already had some knowledge about this kind of numbers. However, the earliest records of an explicit study of prime numbers is due to the Greeks and the allocation of the school of Pythagoras. Euclid's Elements (about 300 BC), contains important theorems about primes, including the demonstration of its infinity the fundamental theorem of arithmetic. Euclid also showed how to construct a perfect number from a Mersenne prime. This issue has been settled in antiquity by Eratosthenes (276-194 BC), the first person, as far as is known to produce tables of prime numbers. As the concept of prime numbers a very important factor in the theory of numbers, types, their theorems, conjectures, hypotheses, sizes, applications and some demonstrations. The Greek Eratosthenes, attributed to a simple method for calculating prime numbers, known today as the sieve of Eratosthenes. Moreover, in modern times, large prime numbers are found on the basis of codes of information security for computers, through tests of primality more sophisticated, such as the AKS primality test.

KEY WORDS: Mathematics, Prime Numbers Known.

SUMÁRIO

1. INTRODUÇÃO

Há muitos anos os números primos atraem a atenção de matemáticos de todo o mundo, por várias razões. Uma delas é a irregular distribuição ao longo da reta numérica. Os números primos aparecem espalhados aqui e ali. São qualificados como misteriosos e indomáveis, pois não parece existir nenhuma regra que determine seu lugar entre os demais números naturais. Se bem que não há uma fórmula que prediga a distância entre um primo e outro.

É atribuído aos pitagóricos (aprox. 550 a. C.) os primeiros estudos sobre os números pares, ímpares, primos, perfeitos, amigos, figurados, etc. Euclides (aprox. 300 a.C.) dedica em sua monumental obra “Os Elementos” alguns livros sobre os pitagóricos, e especialmente, no Livro IX - Proposição 20 demonstra que o conjunto dos números primos é infinito. Daí surge à questão de determinar, dentre os inteiros positivos, todos os números primos até certo número dado. Esta questão também foi resolvida na Antiguidade por Eratóstenes (276-194 a. C.), a primeira pessoa, até onde se sabe, que produziu tabelas de números primos. Ele escrevia inicialmente uma lista com todos os números de 1 a 1000. Em seguida escolhia o primeiro primo, 2, e eliminava da lista todos os seus múltiplos. Passava ao número seguinte que não fora eliminado e procedia também eliminando todos os seus múltiplos, esse método ainda é usado hoje, e é chamado de **“**Crivo de Eratóstenes”. Outro resultado importante de Euclides é a relação entre números primos e números perfeitos, tendo demonstrado, inclusive, que se $2^n - 1$ é primo, então $P_n = 2^n - 1\,(2^n - 1)$ é perfeito.

A MATEMATICA DOS NUMEROS PRIMOS

A História dos Números Primos

Os números primos, e as suas propriedades, foram pela primeira vez estudada pelos antigos matemáticos Gregos.

Os matemáticos da escola de Pitágoras (500 a 300 A.C.) estavam interessados nos números pelas suas propriedades numerologias e místicas. Entendiam a idéia, e revelavam interesse em números perfeitos e amigáveis (um número perfeito é um número cujo resultado da soma dos seus divisores naturais é ele mesmo; por exemplo, o número 6 tem como divisores 1, 2, 3 e 1+2+3=6. Um par de números amigáveis, é por exemplo 220 e 284, e são tais que, os divisores de um somam-se ao do outro e vice-versa).

Quando Os Elementos de Euclides apareceram (cerca de 300 A.C.) já muitos dos resultados importantes sobre números primos tinham sido provados. No livro IX d'Os Elementos, Euclides prova que existem infinitos números primos. Esta é uma das primeiras demonstrações conhecidas a usar o método da contradição, com vista à obtenção de um resultado. Euclides dá-nos também, uma demonstração do Teorema Fundamental da Aritmética - qualquer inteiro pode ser escrito como produto de números primos em essencialmente uma única maneira. Também mostrou que se um número da forma 2^n -1 é primo, então o número desta forma é um número perfeito.

O matemático Euler (1747) mostrou que todos os números pares perfeitos são desta forma. Não é conhecido até à data qualquer número perfeito ímpar.

A 200 A.C. o Grego Erastostenes apresentou um algoritmo para calcular números primos, o Crivo de Erastóstenes.

Segue-se depois um largo período de tempo de interregno, na História dos Números Primos, durante a chamada Idade Negra. O seguinte desenvolvimento na História dos Números Primos é-nos fornecido por Fermat no início do século XVII. Este provou uma especulação conjecturada por Albert Girard, que diz que todo o número primo da forma 4n+1 pode ser escrito de um só modo como soma de dois quadrados e, foi capaz de nos mostrar que qualquer número pode ser escrito como soma de quatro quadrados. Criou um novo método para fatorar números primos grandes. Também provou o que é hoje conhecido como Pequeno Teorema de Fermat (para distinguir do denominado Grande Teorema de Fermat). Seja n um número primo então para qualquer número inteiro a, tem-se que: a^p ºa (mód. p) Tal teorema prova em parte, o que foi chamado de Hipótese Chinesa , que data de cerca de 2000 anos antes, e que diz que um inteiro n é primo, se e só se o número 2^n -2 é divisível por n. A outra metade deste teorema é falsa; vê-se facilmente com o exemplo de que 2^{341}-2 é divisível por 341, e 341=31x11.

O Pequeno Teorema de Fermat é à base de muitos resultados da Teoria dos Números, e de métodos conceitualisadores com vista à determinação de números primos, que ainda hoje são utilizados em larga escala, em computação. Fermat correspondeu-se com outros matemáticos do seu tempo, e em particular com o monge Marin Mersenne. Numa das suas cartas a Mersenne, conjecturou que os números da forma 4^n -1 , F^n (número de Fermat) são sempre primos, mas o resultado falha.

Números desta forma são chamados de Números de Fermat e, só cerca de 100 anos mais tarde é que Euler demonstra que tal tem uma falha: 2^{32} + 1=4294967297 que é divisível por 641 e logo não é primo.

Os Números de Fermat da forma 2^n - 1 também atraiu a atenção, devido à demonstração óbvia de que caso n não seja um número primo, então estes números são compostos, logo favoráveis. Estes são vulgarmente chamados de Números de Mersenne M^n, devido ao estudo que este matemático lhe dedicou. Nem todos os números da forma 2^n -1 com n primo são números primos.

Por exemplo, 2^{11} -1 =2047=23x89 é composto; no entanto tal não foi descoberto até cerca de 1536. Por muitos anos os números desta forma forneceram-nos os maiores números primos. O número M^{19} foi provado como sendo primo por Cataldi em 1588, e este foi o maior número primo por cerca de 200 anos, até que Lucas nos mostrou que M^{127} (que é um número que tem 39 dígitos) é primo; tal número foi o recordista até à era do computador eletrônico. Em 1952 os Números de Mersenne ,M^{521} , M^{607} , M^{1279} , M^{2203} , M^{2281}são descobertos por Robinson com a ajuda dum primitivo computador eletrônico, o que estabelece o inicio da era eletrônica.

Até à data da realização desta página é conhecido um total de 37 Números Primos de Mersenne. O maior conhecido é $M^{3021377}$, que tem 909526 dígitos decimais.

O trabalho de Euler tem também um grande impacto na Teoria dos Números em geral, e na Teoria dos Números Primos em particular. Ele estende o Pequeno Teorema de Fermat e introduz a função-pi de Euler.

Como mencionado já atrás, fatorar o quinto número de Fermat : 2^{32} +1 (F^n), descobre 60 pares de números amigáveis, e conjectura (mas não é capaz de provar) o que é conhecida como a Lei da Reciprocidade Quadrática.
É o primeiro a aperceber-se que a Teoria dos Números pode ser estudada usando as

ferramentas da Análise, e em fazendo tal funda a Análise da Teoria dos Números. Mostra-nos que, não só a conhecida série harmônica (å1/n, com 0£n£¥) é divergente, mas como a série harmônica com n é primo (å1/n, com nÎN, e n primo), também é divergente.

A soma dos n termos da série harmônica cresce logaritmicamente, enquanto a outra série diverge ainda mais lentamente como(log(n)). Isto mostra que somando os inversos de todos os números primos, temos que o mais poderoso dos computadores modernos, nos dá como valor dessa soma cerca de 4, enquanto a série é divergente, isto é converge para infinito.

À primeira vista os números primos parecem não ter uma ordem específica de aparecimento. Por exemplo, em relação aos 100 primeiros números imediatamente antes de 10 000 000 existem apenas 9 números primos, enquanto nos 100 números que se seguem existem apenas 2 números primos. No entanto a uma ainda maior escala, a distribuição de números primos parece ser mais regular.Legendre e Gauss fizeram ambos extensos cálculos sobre a densidade dos números primos. Gauss (que era um prodígio do cálculo) disse a um amigo que sempre que tinha 15 minutos de folga, os ocupava contando os números primos num alcance de 1000 números. No fim da sua vida estimou-se que Gauss tinha contado todos os números primos até 3 milhões.

Legendre e Gauss chegaram ambos à conclusão de que para um n grande a densidade de números primos perto desse mesmo n é semelhante a 1/log(n). Legendre deu uma estimativa para p(n) dos números de primos relacionados com n de p(n)=n/((log(n))-1.08366) enquanto Gauss estimou isso mesmo em termos de

integral logarítmico p(n)= ò 1/log(t) dt (onde o alcance de integração é de 2 a n). Pode ver-se a estimativa de Legendre e compará-la com a estimativa de Gauss.

A conjectura de que a densidade de números primos é 1/log(n) é conhecida como o Teorema dos Números Primos.

Tentativas de provar continuaram pelo século XIX a dentro com progressos notáveis por Chebyshev e Riemann que foram capazes de relacionar o problema com algo semelhante à chamada Hipótese de Riemann : uma conjectura ainda por demonstrar sobre os zeros no plano complexo, de uma função chamada de função-zeta Riemann. O Resultado foi eventualmente provado (usando poderosos métodos da Análise Complexa) por Hadamard e Vallée Poussin em 1896.

Ainda há muitas questões por desvendar (algumas delas que datam de há centenas de anos atrás) relacionadas com números primos...

Quantos números primos existem ?

A resposta a esta questão é-nos dada pelo Teorema Fundamental:

Existem infinitos números primos. Serão dadas nove demonstrações e meia, por famosos e também esquecidos matemáticos, deste Teorema Fundamental. Algumas das demonstrações sugerem-nos desenvolvimentos interessantes, do assunto; outras são apenas astuciosas e curiosas. Existem, é claro, mais provas (mas não em número infinito) da existência de infinitos números primos.

Números Primos

Um número natural é um número primo quando ele tem exatamente dois divisores: o número um e ele mesmo.

Nos inteiros, p ϵ ƶ é um primo se $p \neq 0$, $p \neq 1$, $p \neq -1$, e se $p = ab$ com a, b ϵ ƶ então a= ± 1 ou b= ± 1.

Existem infinitos números primos, como demonstrado por Euclides por volta de 300 a.C..

A propriedade de ser um primo é chamada "primalidade", e a palavra "primo" também é utilizada como substantivo ou adjetivo. Como "dois" é o único número primo par, o termo "primo ímpar" refere-se a todo primo maior do que dois.

Se um número inteiro tem módulo maior que um e não é primo, diz-se que é composto. Por convenção, os números 0, 1 e -1 não são considerados primos nem compostos.

O conceito de número primo é muito importante na teoria dos números. Um dos resultados da teoria dos números é o Teorema Fundamental da Aritmética, que afirma que qualquer número natural diferente de 1 pode ser escrito de forma única (desconsiderando a ordem) como um produto de números primos (chamados fatores primos): este processo se chama decomposição em fatores primos (fatoração).

Exemplos de decomposições:

- 4 = 2 x 2
- 6 = 2 x 3
- 8 = 2 x 2 x 2
- 9 = 3 x 3
- 10 = 2 x 5
- 472.342.734.872.390.487 = 3 x 7 x827 x 978.491 x 27.795.571

Os números que tem 2 divisores só podem ser dividido de forma exata pela unidade e por si mesmos. Entre os 10 primeiros números naturais encontramos 4 primos: 2, 3, 5 e 7. De 1 ao 100 há 25 primos. De 1 a 1000 há 168 e à medida que avançamos pela reta se fazem cada vez mais escassos, sendo sua distribuição muito irregular. Os números primos são importantes porque são os átomos da Matemática. Todos os demais números se constroem a partir deles. Os números primos são infinitos como demonstrou Euclides no ano 300 a.C., os primos menores de 10 são extraordinários: o 2 é o único primo par. O 2 e o 3 são os únicos primos contínuos. O 5 é o único terminado em 5. Por último: 3, 5 e 7, formam a única tríade de primos gêmeos em toda a reta numérica. As lacunas ou brechas são setores da reta numérica onde não aparece nenhum número primo. Os números primos não podem ser decompostos num produto de fatores menores que eles.

O CRIVO DE ERATÓSTENES

Eratóstenes viveu no século III a.C, em uma colônia grega na Líbia chamada Cyrene. Dentre suas contribuições, destaca-se um método para a determinação de números primos, o qual é conhecido como o crivo de Eratóstenes que é um antigo e efetivo de método para achar números primos. Consiste em uma tábua de números naturais dispostos em colunas.

Exemplo 01 – Para determinar os números primos menores que 100, o primeiro passo é listar, em ordem crescente, todos os números naturais de 2 até 100.

Em seguida, retiramos todos os números maiores que 2 e múltiplos de 2 (4, 6, 8, ...), os quais não são primos, porque são números pares.

Os próximos números a serem retirados são os múltiplos de 3 maiores que 3 (9,15,21,..); os quais também não são primos, pois são divisíveis por 3.

Continuando, retiramos os múltiplos de 5 maiores que 5 e, finalmente, os múltiplos de 7 maiores que 7. Os números que restarem são todos os números primos menores do que 100.

Note-se, que não é necessário retirar os múltiplos de 11, uma vez que o primeiro múltiplo de 11 a ser retirado seria o número 11.11 = 121, o qual é maior que 100.

Em linhas gerais, quando utilizamos o crivo de Eratóstenes para encontrar todos os números primos menores que um número natural n, retiramos somente os números múltiplos dos primos menores que a raiz quadrada de n.

Exemplo 02 - N = 101

Primeiro se apagam todos os múltiplos de 2. Logo se apagam todos os múltiplos do seguinte número não apagado anteriormente e assim por diante. Os números que ficarem sem apagar são os números primos. Esse crivo serve para determinar todos os números primos até um dado número N.

Seguem-se os seguintes passos:

1 - Escrevem-se todos os números até 101

2 - Cortam-se, com um traço, todos os múltiplos de 2;

3 - A cada passo seguinte cortam-se todos os números múltiplos do seguinte menor número restante de p, que seja maior do que p.

4 - É suficiente fazê-lo até $p^2 < 101$.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~

31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101									

Embora todos os múltiplos de 2, 3, 5, 7 < $101^{½}$ sejam cortados, resta-nos o número 53, que é primo, pois ficou sem ser cortado.

Então os números primos até 101 são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101.

O Teorema Fundamental da Aritmética

"Todo número composto $n > 1 \in N$ pode ser escrito como um produto de números primos". Assim, $\exists\ p_1, p_2, p_3, ..., p_n \in P$ tais que $n = p_1.p_2.p_3. ....p_n$.

Alguns exemplos:

4 = 2.2

15 = 3.5

20 = 2.2.5

28 = 2.2.7

144 = 2.2.2.2.3.3

200 = 2.2.2.5.5

E assim por diante.

Demonstração

A prova será feita por indução.

Se k = 2, o resultado é imediato, então considere que o mesmo vale para todo número inteiro menor que k = n.

Supondo que existem duas decomposições para i inteiro n, ou seja, $n = p_1.....p_r = q_1.....q_s$, segue que algum q_j é múltiplo de p_1. Como a ordem dos fatores não é importante, pode-se supor que j = 1.

Neste caso, segue que $p_1 = q_1$, pois $p_1 \neq 1$ e os únicos divisores de q_1 são 1 e ele próprio. Logo, $n = p_1.....p_r = q_1.....q_s$ implica que $m = p_2.....p_r = q_2.....q_s$. Certamente m < n, então pela hipótese de indução, m possui uma fatoração única, onde r = s e $p_j = q_j$, para cada índice j. Assim a fatoração de n é única.

Corolário

Todo $n \in N^*$ pode ser escrito como $n = p_1^{e_1} \cdot ... \, p_r^{e_r}$, com $p_1 < p_2 < ... < p_r$ e $e_j \geq 1$. Esta é chamada de forma padrão da decomposição em fatores primos.

Outra forma de escrita é $n = \prod_p p^{e_p}$, com $e_j = 0$, exceto para uma quantidade finita de p. A constatação da verdade dessas afirmações é elementar.

Aplicação

A partir dessa notação pode-se definir uma função $u_p : N \to N$ escolhendo $u_p (n) = e_p$. Verifica-se que a função acima definida goza das seguintes propriedades:

1. $u_p (m.n) = u_p (m) + u_p (n)$
2. $u_p (m + n) \geq \min(u_p (m), u_p (n))$

Essa função oferece uma forma "elegante" de se fazer certas demonstrações. Por exemplo, a irracionalidade de $\sqrt{2}$ é provada assim:

Demonstração:

Se $\sqrt{2}$ fosse racional, poderia ser escrito como $\sqrt{2} = \frac{a}{b}$, sendo que $a, b \in Z$, e $b \neq 0$.

Neste caso, seria verdade que $\left(\frac{a}{b}\right)^2 = 2$, ou seja, $a^2 = 2b^2$. Aplicando a função υ_2 em ambos os membros, segue que:

$$2\upsilon_2 (a) = \upsilon_2 (a^2) = \upsilon_2 (2b^2) = \upsilon_2 (2) + 2\upsilon_2 (2b) = 1 + 2\upsilon_2 (b)$$

No entanto, essa igualdade é possível, pois o primeiro membro é um número par, e o último é ímpar. Logo, $\sqrt{2}$ só pode ser irracional.

TEOREMAS DOS NÚMEROS PRIMOS

Sabe-se que, à medida que avançamos na seqüência dos números inteiros, os primos tornam-se cada vez mais raros. Isto levanta duas questões:

1. O conjunto dos números primos seria finito ou infinito?

2. Dado um número natural *n*, qual é a proporção de números primos entre os números menores que *n*?

A resposta à primeira questão é que o conjunto dos primos é infinito, um resultado conhecido na parte central dos Elementos de Euclides, que lida com as propriedades dos números. Na proposição 20, Euclides explica uma verdade simples, porém fundamental sobre os números primos: existe um número infinito deles. Pode-se demonstrar, em notação moderna, da seguinte forma:

Suponha, por absurdo, que o número de primos seja finito e sejam p_1, p_2, p_3, ..., p_n os primos. Seja P o número tal que:

$$\prod_{i=1}^{n} p\,i + 1\,,$$

P = onde $\prod$ denota o produtório.

Se P é um número primo, é necessariamente diferente dos primos p_1, p_2, p_3, ..., p_n, pois sua divisão por qualquer um deles tem um resto de 1.

Por outro lado, se P é composto, existe um número primo q tal que q é divisor de P.

Mas obviamente $q \neq p_1, p_2, p_3, ..., p_n$. Logo existe um novo número primo.

Há um novo número primo, seja *P* primo ou composto; este processo pode ser repetido indefinidamente, logo há um número infinito de números primos.

Outra prova envolve considerar um número inteiro n > 1. Temos n + 1 que, necessariamente, é coprimo de n (números coprimos são os que não tem nenhum fator comum maior do que 1). Provamos isto imaginando que a divisão do menor pelo maior tem resultado 0 e resto n e do maior pelo menor tem resultado 1 e resto 1. Assim, n(n + 1) tem, necessariamente, ao menos dois fatores primos.

Tomemos o sucessor deste, que representamos como n(n + 1) + 1. Pelo mesmo raciocínio, ele é coprimo a n(n + 1). Ao multiplicar os dois números, temos [n(n + 1)] * [n + (n + 1) + 1]. Como um de seus fatores tem pelo menos dois fatores primos diferentes e é coprimo ao outro, o resultado da multiplicação tem pelo menos três fatores primos distintos. Este raciocínio também pode ser infinitamente estendido.

A resposta para a segunda pergunta acima é que essa proporção é aproximadamente $\frac{\mathbf{n}}{\mathbf{ln(n)}}$, onde ln é o logaritmo natural.

Para qualquer inteiro *k*, existem *k* inteiros consecutivos todos compostos. O produto de qualquer seqüência de *k* inteiros consecutivos é divisível por *k!*

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

Todo inteiro maior que 1 pode ser representado de maneira única como o produto de fatores primos.

A função π (x) dos números primos

A função π (x) dos números primos é definida como a quantidade de números primos menores ou iguais a x, ou seja: π (x) = |{p $\in$ P | p ≤ x}|.

Por exemplo:

a) Se $0 \leq x < 2$, temos que $\pi(x) = 0$.

b) Se $2 \leq x < 3$, temos que $\pi(x) = 1$.

c) Se $3 \leq x < 7$, temos que $\pi(x) = 2$.

Existe um teorema, proposto por vários matemáticos, dentre eles Legendre e Gauss, mas cuja demonstração completa só foi encontrada em 1896, por de la Vallée Poussin e Hadamard de maneira independente, que é expresso da seguinte forma: $\lim_{x\to\infty}\left(\frac{\pi(x)}{\frac{x}{\ln|x|}}\right) = 1$, ou seja, quando temos um x muito grande, a quantidade de números primos é dada por uma excelente aproximação de $\frac{x}{\ln|x|}$

A Conjectura de Goldbach

Christian Goldbach (1690-1754) estabeleceu a seguinte pergunta que até hoje não pôde ser decidida:

Todo número par $n > 4$ é soma de dois primos ímpares.

Exemplo:

$6 = 3 + 3$, $8 = 3 + 5$, $10 = 7 + 3 = 5 + 5$, $12 = 7 + 5$...,

$100 = 97 + 3 = 89 + 11 = 83 + 17 = 71 + 29 = 59 + 41 = 53 + 47$ ....

Pelo teorema de Tchebychef existe sempre um primo entre qualquer número e seu dobro. Por outro lado, é uma observação simples que existem intervalos de comprimento arbitrário n, livre de números primos, como mostra

Proposição

Para todo $n \in N$ existe um $k_n \in N$ tal que os números consecutivos,

$$k_n + 1, k_n + 2, k_n + 3, ..., k_n + n$$

são todos compostos.

Demonstração: Dado $n \in N$, escolhemos $k_n = (n + 1)! + 1$. Como 2,3,4, ..., (n + 1) todos dividem (n + 1)!, obtemos

$$2| (n + 1)! + 2 = k_n + 1,$$

$$3| (n + 1)! + 3 = k_n + 2,$$

$$\vdots \quad \vdots \quad \vdots$$

$$n| (n + 1)! + n = k_n + (n - 1),$$

$$(n + 1)| (n + 1)! + (n + 1) = k_n + n,$$

mostrando que esses números são compostos.

Teorema de Tchebychef

Para $m \geq 2 \in N$, temos que sempre existe um primo **p** tal que **m < p < 2m**. Logo, para o enésimo primo p_n vale a estimativa: $p_n \leq 2^n$.

Seja $n \in N$ um número ímpar.

- n é um número primo, se e somente se, $n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$ é a única decomposição de n como diferença de dois quadrados, dado que $\left(\frac{n \pm 1}{2}\right)$ é um número inteiro.

Seja n = a.b, tal que $1 \leq b \leq a \leq n \in N$. Seja a = x + y e b = x – y.

Logo, $n = (x + y)(x – y) \Rightarrow n = x^2 – y^2$.

Assim, n possui tantas decomposições distintas como diferença de dois quadrados quantas decomposições multiplicativas distintas ele admite.

TIPOS DE NÚMEROS PRIMOS

Os primos de Fermat

São obtidos pela relação $p_n = 2^{2^n} + 1$, para $n \in N = N^* \cup \{0\}$. Pierre de Fermat (1601 – 1665) acreditou que essa fórmula geraria apenas números primos para todo e qualquer $n \in N$. Mas Euler (1707 – 1783), outro fantástico matemático, provou que essa indução é falsa para n = 5.

Demonstração:

$n = 0 \Rightarrow p = 2^{2^0} + 1 = 3$

$n = 1 \Rightarrow p = 2^{2^1} + 1 = 5$

$n = 2 \Rightarrow p = 2^{2^2} + 1 = 17$

$n = 3 \Rightarrow p = 2^{2^3} + 1 = 257$

$n = 4 \Rightarrow p = 2^{2^4} + 1 = 65.537$

Todos são números primos. Mas para n = 5, temos:

$n = 5 \Rightarrow p = 2^{2^5} + 1 = 2^{32} + 1 = 4.294.967.297 = 641 \times 6.700.417$, que constitui um número divisível por 641.

Os primos de Sophie Germain

Um número primo p é um número primo de Sophie Germain se 2p + 1 é também primo. São famosos porque Sophie Germain (1776 – 1831), uma exímia matemática e teórica dos números, provou que o *Último Teorema de Fermat* é verdadeiro para estes números. A existência de um número infinito de tais números primos é uma conjectura, ou seja, uma afirmação não provada.

Os primeiros primos de Sophie Germain são (sequência A005384 em OEIS): 2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233…

O maior número primo de Sophie Germain conhecido até à data é o número $7068555.2^{121301} - 1$ que tem 36523 dígitos e foi descoberto em 8 de Janeiro de 2005.

Uma sequência {p, $2p + 1$, $2(2p + 1)+1$, ...} de primos de Sophie Germain também recebe o nome de cadeia de Cunningham de primeira classe.

Os primos de Mersenne

Marin Mersenne (1588 – 1648) foi um frei franciscano que dedicou grande parte da sua vida em pesquisas matemáticas. Correspondia-se com grandes matemáticos da época, incluindo Fermat. Em um trabalho intitulado “Cognitata Physico-Mathematica”, Mersenne afirmou que $2^m - 1$ é primo para m = {2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257}. Em um trabalho de 1947, mostrou-se que para m = {61, 89, 107}, $2^m - 1$ também é primo, e que $2^{257} - 1$ é composto. Atualmente o maior número primo encontrado é $2^{43.112.609} - 1$ descoberto no dia 23 de agosto de 2008, é o primo de Mersenne de número 46 e tem 12.978.189 dígitos.

Os primos de Wieferich

São números primos *p* onde p^2 divide 2^{p-1} - 1. Foram descritos por Wieferich em 1909 e existem apenas dois conhecidos: 1093 e 3511.

Os primos de Wilson

São os primos *p* onde p^2 divide (*p* - 1)! + 1. Os únicos conhecidos são 5, 13 e 563.

Os primos fatoriais

Têm a forma *n*! ± 1. n! - 1 é primo para n = 3, 4, 6, 7, 12, 14, 30, 32, 33, 38, ... e n! + 1 é primo para n = 1, 2, 3, 11, 27, 37, 41, 73, 77, 116, ...

Os primos primorial

O primorial de um número natural n maior que 1 é denotado por n# e é definido como o produto de todos os números primos menores ou iguais a n. O primorial de 1 é definido como sendo igual a unidade.

Exemplos

1# = 1

2# = 2

3# = 2.3 = 6

4# = 2.3 = 6

5# = 2.3.5 = 30

6# = 2.3.5 = 30

7# = 2.3.5.7 = 210

Estimativa de crescimento para o primorial

Para todo $n \geq 1$, $n\# < 4^n$. A demonstração se faz por indução matemática.

Base:

$1\# = 1 < 4^1$

$2\# = 2 < 4^2$

Indução

n > 2, n é par:

$n\# = (n - 1)\# < 2n - 1 < 2^n$

n > 2, n é impar, então se escreve n = 2m + 1

$$4^m = \frac{1}{2}(1+1)^{2m+1} = \frac{1}{2}\sum_{k=0}^{2m+1}\binom{2m+1}{k} > \frac{1}{2}\left(\binom{2m+1}{m} + \binom{2m+1}{m+1}\right) = \binom{2m+1}{m}$$

Como cada número primo *p*, $m + 1 < p \leq 2m + 1$ é divisor de $\binom{2m+1}{m+1}$, temos que:

$$\prod_{p> m+1}^{p \le 2m+1} p \le \binom{2m+1}{m+1} < 4^m$$

Agora, podemos estimar:

$n\# = (2m+1)\# = (m+1)\# \prod_{p> m+1}^{p \le 2m+1} p < 4^{m+1}\, 4^m = 4^{2m+1} = 4^n$

E o resultado segue.

Hipótese de Riemann

O matemático Bernhard Riemann (1826 – 1866) foi uma figura fantástica no campo da matemática. Contribuiu para diversas áreas do conhecimento matemático, como a análise e a geometria diferencial. A hipótese de Riemann foi publicada pela primeira vez em 1859, e declara que os zeros não-triviais da *função zeta de Riemann* pertencem todos à "linha crítica":

Função zeta de Riemann: $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, para Re(s) >1. - onde s é um número complexo na forma s = a + bi.

- os zeros triviais da função zeta de Riemann são os inteiros negativos pares - 2, - 4, - 6,…

- todos os zeros da função zeta que não são números reais estarão na reta vertical x = $\frac{1}{2}$. Essa reta é a chamada reta crítica.

A hipótese de Riemann sobre os números primos é de tal importância que tem intrigado os matemáticos há mais de 150 anos. A hipótese é um dos poucos problemas não resolvidos do problemas de Hilbert e foi colocado como problema número 1 de Smale. É tão difícil que em 2000 o Clay Mathematics Institute ofereceu

um prêmio de 1 milhão de dólares a quem prová-lo. Sendo que o Prof. Louis de Branges de Bourcia, matemático da Universidade Purdue em Lafayette, Indiana, EUA, afirma ter conseguido prová-la, e submeteu sua "prova" para publicação.

OS MAIORES NÚMEROS PRIMOS CONHECIDOS

Primos titânicos

Nos anos 80, Samuel Yates iniciou uma lista dos "Maiores Primos Conhecidos" e criou o nome primo titânico para designar qualquer número primo com 1.000 ou mais dígitos. Denominou também de titãs aqueles que provaram a primalidade destes números.

Hoje em dia, uma infinidade de primos titânicos são conhecidos. Entretanto, na época em que Yates definiu os primos titânicos, tinha-se conhecimento de apenas alguns poucos.

Primos gigantes

Cerca de dez anos mais tarde, Yates designou como primo gigante todo número primo que possuísse 10.000 ou mais dígitos. Nos anos 90 estes primos eram bastante raros. Atualmente, vários deles são conhecidos.

Megaprimos

São números primos que possuem no mínimo um milhão de dígitos. Vários são conhecidos .

APLICAÇÕES DOS NÚMEROS PRIMOS

Números primos extremamente grandes, maiores do que 10100, são usados em vários algoritmos de criptografia de chave pública. Também são usados para tabelas hash e geradores de números pseudorandômicos.

NÚMEROS PRIMOS ENTRE SI

Dois números inteiros são ditos primos entre si quando não existir um divisor maior do que 1 que divida ambos. Isto significa que o máximo divisor comum (ou MDC) dos primos entre si é igual a 1.

Por exemplo, 12 e 13 são primos entre si; porém, 12 e 14 não são, porque ambos são divisíveis por 2.

Um conjunto de números inteiros é chamado de mutuamente primo se não existir um inteiro que divida todos os elementos. Por exemplo, os inteiros 30, 42, 70 e 105 são mutuamente primos. Entretanto, aos pares, não são primos entre si.

Esta definição é transferida para outras áreas. Por exemplo, dois polinômios com coeficientes inteiros são primos entre si se não houver um polinômio não-constante que divida ambos.

DEMONSTRAÇÕES

Serão dadas quatro demonstrações, por famosos e também esquecidos matemáticos, deste Teorema Fundamental. Algumas das demonstrações sugerem-nos desenvolvimentos interessantes, do assunto; outras são apenas astuciosas e curiosas. Existem, é claro, mais provas (mas não em número infinito) da existência de infinitos números primos.

Demonstração de Euclides:

Suponhamos que $p_1 = 2 < p_2 = 3 < ... < p_r$ são todos números primos. E seja $P = p_1.p_2.....p_n + 1$ e p um número primo que divida P; então p não pode ser nenhum dos $p_1, p_2, ..., p_n$, senão p dividiria a diferença $P - p_1.p_2.....p_r = 1$ o que é impossível. Logo este número primo p é ainda outro número primo, e $p_1, p_2, ..., p_r$ não serão todos os números primos existentes.

Escreveremos a sucessão infinita e crescente de números primos da forma

$p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, ...,$ p_n, ...

A demonstração de Euclides é muito simples; no entanto, não nos dá qualquer informação sobre o novo número primo, unicamente de que ele é quanto muito igual ao número P, mas pode bem ser que seja menor que este.

Para cada número primo p, seja p# definido pelo produto de todos os números primos q, tais que q é menor ou igual a p.

Seguindo a sugestão de Dubner, p# pode ser chamado de primordial de p.

As respostas às seguintes questões são ainda desconhecidas:

- Existem infinitos números primos p para os quais p# + 1 é um número primo?

- Existem infinitos números compostos p para os quais p# + 1 é um número composto?

Recorde: 13649# + 1 é o maior número primo da forma p# + 1; tem 5862 dígitos e foi descoberto por Dubner em 1987, que também identificou p = 11549, 4787, 4547 e 3229 com a mesma propriedade.

No entanto, trabalhos anteriores de, Borning (1972), Templer (1980), e Buhler, Crandall e Penk (1982) estabeleceram que p# + 1 é um número primo para p = 2, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, e que p# + 1 é um número composto para todos os outros p < 11213, com p pertencente a N.

Demonstração de Euler

Base da demonstração de Euler

Esta é uma demonstração indireta, que em senso comum parece ser pouco natural; mas por outro lado, como indicaremos, conduz-nos a importantes desenvolvimentos. Euler mostrou que devem existir infinitos números primos pelo fato de certa expressão formada por todos os números primos ser infinita. Se p é um número primo, então 1/p < 1; conseqüentemente, a soma da série geométrica é: $S1/p^k = 1/ (1 - 1/p)$. Do mesmo modo, se q é outro número primo então, $S1/q^k = 1/ (1 - 1/q)$. Multiplicando: $1 + 1/p + 1/q + 1/p^2 + 1/q^2 + ... = [1/(1-1/p)].[1/(1-1/q)]$. Mais explicitamente, a parte esquerda é a soma dos inversos de todos os números naturais da forma $p^h.q^k$, (com h maior ou igual que zero e k maior ou igual que zero), cada um contado uma única

vez, porque cada número natural tem uma única fatorização como produto de números primos. Esta simples idéia é à base da demonstração de Euler

Demonstração de Euler:

Suponhamos que p_1, p_2, ..., p_n são todos números primos. Para cada j = 1, ..., n, $S1/pj^k = 1/ (1 - 1/pj)$. Multiplicando estas n igualdades obtemos: $P(S\ 1/pj^k = 1/ (1 - 1/pj))$ = P1/ (1 - 1/pj) (com 1£ j £n) e a parte esquerda é a soma dos inversos de todos os naturais, cada um contado uma e uma só vez - o que advém do teorema que diz que cada número natural é igual, de um só modo, a produto de números primos. Mas a série, S 1/n é divergente (série harmônica), sendo uma série de termos positivos, a ordem da sua soma é irrelevante, logo a parte esquerda é infinita quando a parte direita é claramente finita. Isto é absurdo.

Demonstração de Polya

A demonstração de Polya usa a seguinte ideia: É suficiente encontrar uma sucessão natural de números 1 < a1 < a2 < a3 < ... que sejam primos relativos dois a dois (isto é sem factores primos em comum). Logo, se p1 é um primo que divida a1, se p2, é um primo que divida a2, etc., então p1, p2, ..., são todos diferentes. Nesta demonstração os números an são escolhidos como sendo os números de Fermat, $\mathbf{F}^{n} = 4^{n} + 1$ (n³ 0). De facto, é fácil de ver por indução em m, que $\mathbf{F}^{m} - 2 = \mathbf{F}^{0}.\mathbf{F}^{1}...\mathbf{F}^{m-1}$; conseqüentemente, se n < m, então $\mathbf{F}^{n}$ divide $\mathbf{F}^{m} - 2$. Se um primo p dividisse $\mathbf{F}^{n}$ e $\mathbf{F}^{m}$, então dividiria $\mathbf{F}^{m} - 2$ e $\mathbf{F}^{m}$, e por isso também 2, logo p = 2. Mas $\mathbf{F}^{n}$ é impar, conseqüentemente não divisível por 2. Isto mostra-nos que os números de Fermat são primos relativos dois a dois.

Demonstração de Kummer

Suponhamos que existe apenas um número finito de primos p1 < p2 < ... < pr. Seja N = p1.p2.....pr>2 . O inteiro N - 1, sendo produto de números primos (composto), tem um divisor primo pi em comum com N; logo, pi divide N - (N - 1) = 1, o que é absurdo.

Demonstração de Fursthenberg

A demonstração de Fursthenberg é uma prova engenhosa, baseada em idéias topológicas, que apareceu em 1955.

Vamos demonstrar topologicamente que existe um infinito número de números primos.

Primeiro introduzimos uma topologia num espaço S de números inteiros, usando as progressões aritméticas (de menos infinito a mais infinito) como base. Não difícil verificar que de fato, que esta noção assim dada, suporta um espaço topológico. De fato, dentro desta topologia, podemos mostrar que S é normal, logo metrizável. Cada progressão aritmética é simultaneamente aberta e fechada. Como resultado a união de qualquer número finito de progressões aritméticas é fechada. Considere-se agora um conjunto A que é igual à união de todos os conjuntos Ap, onde Ap consiste de todos os múltiplos de p, e p pertence ao conjunto dos números primos maiores ou iguais a 2. Os únicos números que não pertencem a A são -1 e 1, e como o conjunto {-1, 1}, é um conjunto fechado, A não pode ser fechado. Conseqüentemente, A não é uma união finita de conjuntos fechados o que prova que existe um número infinito de números primos.

NÚMEROS PRIMOS EM PROGRESSÃO ARITMÉTICA

Sabemos que um número inteiro positivo é primo se ele é divisível apenas por ele mesmo além do 1. Os números primos desempenham um papel fundamental na Aritmética, análogo ao papel dos átomos na estrutura da matéria, isto é, os números inteiros que não são números primos podem ser expressos como produto de números primos. Portanto, qualquer número inteiro maior que 1 ou é um número primo, ou é expresso como um produto de números primos.

Embora a noção de número primo, no sentido acima, pareça óbvia, em geral, questões envolvendo números primos não são fáceis de serem respondidas no atual estágio da matemática. Por exemplo, todo número ímpar se expressa na forma $4x + 1$ ou $4x + 3$; portanto, perguntamos quais são os primos da forma $4x + 1$ e quais são os primos da forma $4x + 3$. *Será que se gerarmos as seqüências numéricas da forma acima, substituindo-se x por inteiros positivos, as seqüências resultantes apresentarão um número infinito de números primos*?

Euclides de Alexandria (aproximadamente 300 A.C.) deu uma demonstração bastante engenhosa de que existe um número infinito de números primos. O mesmo argumento dado por Euclides pode ser utilizado para se demonstrar a infinidade de primos da forma $4x + 3$. Como 2 é o único primo par, o conjunto dos números primos ímpares se divide em duas famílias:

i) 5, 13,17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173...;

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

Onde a primeira seqüência de números se refere aos primos da forma $4x + 1$ e a segunda aos primos da forma $4x + 3$. Vamos demonstrar que existem infinitos primos do tipo $4x + 3$ utilizando o método de Euclides que demonstra a existência de infinitos primos.

De fato, suponhamos que existisse um número finito de números primos da forma $4x + 3$; vamos denominá-los $q_1, q_2, q_3, \ldots, q_n$. Considere o inteiro positivo: $N = 4 q_1.q_2.q_3. \ldots .q_n - 1 = 4 q_1.q_2.q_3. \ldots .q_n - 4 + 3 = 4 (q_1.q_2.q_3. \ldots .q_n - 1) + 3$ e seja $N = r_1.r_2.r_3. \ldots .r_M$ a sua decomposição em números primos. Como N é um inteiro ímpar, segue-se que r_k é diferente de 2, para todo k, e cada r_k é, portanto, da forma $4x + 1$ ou $4x + 3$. Contudo, o produto de dois ou mais inteiros da forma $4x + 1$ resulta em um inteiro também dessa forma, isto é, $(4m + 1).(4n + 1) = 16mn + 4m + 4n + 1 = 4(mn + m + n) + 1 = 4z + 1$.

Sendo assim, segue-se que N possui pelo menos um fator primo da forma $4x + 3$, digamos $r_i = 4x + 3$.

Agora, afirmamos que r_i não é um elemento da nossa lista original e finita de números primos: $q_1, q_2, q_3, \ldots, q_n$. De fato, caso contrário teríamos $r_i = q_j$, para algum primo q_j da nossa lista original de primos e, então, r_i dividiria o produto $q_1.q_2.q_3.\ldots.q_n$. Por outro lado, sendo r_i um fator de N, r_i divide $N - 4 q_1.q_2.q_3. \ldots .q_n = -1$. Logo, r_i divide -1. Sendo assim, concluímos que existe um número infinito de primos da forma $4x + 3$, pois, assumir que existe um número finito de primos da forma $4x + 3$ nos leva a uma contradição.

A pergunta seguinte seria: existe um número infinito de primos da forma 4x + 1? A resposta é afirmativa, porém devemos utilizar um outro argumento. Uma situação semelhante surge em relação às seqüências de números da forma 6*x* + 1 e 6*x* + 5.

Observe que se gerarmos a seqüência de números da forma 4*x* + 3:

3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63, 67, 71, 75, 79, 83, 87, ... ,

a diferença entre um termo da seqüência e o seu antecessor é sempre igual a 4.

O mesmo ocorre em relação às seqüências da forma 4*x* + 1, 6*x* + 1 ou 6*x* + 5. De fato, temos a seguinte definição: “uma Progressão Aritmética é uma seqüência de números inteiros em que a diferença entre um termo (a partir do 2º.) e o termo antecedente é sempre a mesma”.

Será que o fato de existirem infinitos primos em algumas progressões aritméticas, como as citadas acima, pode ser generalizado?

Observe que as progressões citadas acima são da forma *b* + *ax* onde *a* e *b* são fixados e *x* = 0, 1, 2, 3, 4, 5, ..., isto é, elas são da forma: *b*, *b* + *a*, *b* + 2*a*, *b* + 3*a*, *b* + 4*a*, ...

Se *a* e *b* possuem um fator comum, então a progressão aritmética não contém números primos, pois todo elemento da progressão tem esse fator. Por exemplo, consideremos a progressão aritmética dada por 6 + 2*x*, isto é,

6, 8, 10, 12, 14, 16, 18, 20, 22, 24, ...

Observe que 2 é fator comum de 2 e de 6, e todo termo da progressão tem o número 2 como fator. Esse fato sugere que devemos considerar progressões *b* + *ax* em que *a* e *b* sejam primos entre si para obtermos um número infinito de primos da forma especificada *b* + *ax*. Parece que o matemático Legendre foi o primeiro a perceber a importância dessa questão e, em 1808, publicou a seguinte conjectura:

"*Se* $a \geq 2$ *e* $b \neq 0$ *são inteiros positivos e primos entre si, então existe uma infinidade de números primos na progressão aritmética:* b, $b + a$, $b + 2a$, $b + 3a$, ..."

Essa conjectura se transformou em um teorema de grande importância e foi demonstrada por Dirichlet em 1837. Esse resultado foi monumental por uma série de razões. Dirichlet baseou-se na idéia original de Euler para demonstrar a infinitude dos primos. Foram utilizados métodos analíticos revolucionários tais como séries infinitas, convergência de séries, limites, logaritmos, etc., e muitos outros conceitos até então estranhos à teoria dos números inteiros. A demonstração de Dirichlet é considerada como uma das primeiras aplicações importantes de métodos analíticos em teoria dos números e proporcionou novas linhas de desenvolvimento. As idéias subjacentes aos argumentos de Dirichlet são de um caráter bem geral e foram fundamentais no desenvolvimento do trabalho subseqüente de aplicação de métodos analíticos em teoria dos números.

Em 1949, o matemático Atle Selberg deu uma demonstração elementar do teorema de Dirichlet, análoga à demonstração que dera anteriormente do teorema do número primo.

Dirichlet também demonstrou que qualquer forma quadrática em duas variáveis, isto é, qualquer forma do tipo $ax^2 + bxy + cy^2$ onde a, b, c, são primos entre si, geram uma infinidade de primos. Não se sabe muito sobre outras formas que gerem infinitos números primos.

Por outro lado, podemos demonstrar que não existe progressão aritmética em que todos os termos são números primos. Até o século passado, um velho problema

em aberto consistia em se determinar uma progressão aritmética arbitrariamente longa, porém finita em que todos os termos fossem números primos.

CONCLUSÃO

O presente trabalho teve como objetivo principal apresentar a história da matemática dos números primos e analisam sua importância para o entendimento das sequencias numéricas. Pois a história da matemática dos números primos, e conhecidos pela humanidade há muito tempo.

No entanto em todas as etapas do trabalho tentamos demonstrar de maneira clara e objetiva, as principais características e a importância da história da matemática dos números primos, para os nossos conhecimentos através de pesquisas e sites na internet.

A matemática em si e um grande desafio é um aprendizado que requer desempenho total, e por isso devem usados métodos que auxiliem no desenvolvimento lógico dos alunos, que estão sendo avaliados através do conteúdo administrado. Pensando nisso, e nas questões norteadoras para a manifestação do conhecimento matemático, foram colocados em estudo vários aspectos relacionados com o surgimento e suas demonstrações.

Saber e conhecer a origem dos números primos auxilia na transição de conhecimento, assim possibilitando compreender a importância da matemática para o processo de desenvolvimento escolar e comunitário das ciências exatas, e a sua funcionalidade nas relações problemáticas nos dias atuais para uma melhor existência humana. Por outro lado, nos tempos atuais, os grandes números primos são encontrados com base dos códigos de segurança de informação para computadores, através de testes de primalidade mais sofisticados .

BIBLIOGRAFIA

http://www.somatematica.com.br/coluna/gisele/16072003.php

http://educacao.uol.com.br/matematica/uit1692u20.jhtm

http://www.somatematica.com.br/fundam/primos. ph

http://pt.wikipedia.org/wiki/Teorema_do_n%C3%BAmero_primo

http://pt.wikipedia.org/wiki/N%C3%BAmero_primo_de_Sophie_Germain

http://pt.wikipedia.org/wiki/Primo_de_Mersenne

http://www.uniandrade.br/simposio/pdf/mat104.pdf

http://www.somatematica.com.br/coluna/gisele/27102004.php

http://www.projetozk.ufjf.br/base_p/ensaios/ensaio3/ant_crivo.htm

http://www.educ.fc.ul.pt/icm/icm98/icm12/infinitos.htm

http:www.profcardy.com/cárdicas/tirateima.php?id=2