FALANDO MAIS DOS NÚMEROS PRIMOS: DESAFIOS, PREMIOS, UTILIDADES E MISTERIOS!

Prof. Gustavo Benitez Alvarez

Universidade Federal Fluminense – UFF/EEIMVR, Brasil

benitez.gustavo@gmail.com

III ENCONTRO DE ENGENHARIA DO SUL FLUMINENSE

AGENDA ACADÊMICA 2013

SEMANA NACIONAL DE CIÊNCIA E TECNOLOGIA

Porque esta Palestra?

Na Agenda Acadêmica de 2009 apresentei uma palestra com título:

"NÚMEROS PRIMOS TÊM UTILIDADE? ALGUMAS QUESTÕES ELEMENTARES, DIFÍCEIS E MISTERIOSAS"

Motivado pelo Prof. Nirzi e por uma notícia que percorreu o mundo a finais de 2008.

"Cientistas encontram número primo com quase 13 milhões de dígitos (Notícia publicada 29/09/2008 no O Globo On-line, mais detalhes ver BBC Brasil)."

Esta façanha seria recompensada com US$ 100.000,00 pela Electronic Frontier Foundation.

Desde 1996 existe o projeto GIMPS - Great Internet Mersenne Prime Search, que une esforços de profissionais e amadores de todo o mundo para encontrar números primos de Mersenne grandes.

Em que consiste este premio? Como posso participar? Quem é esse Mersenne?

Calma, vamos aos poucos e chegaremos algum lugar!

Em que consiste este premio?

- A Electronic Frontier Foundation (EFF) oferecia um prêmio de **US$ 100.000,00** para o primeiro que conseguisse encontrar um número primo de **Mersenne** (2^p-1) com mais de 10 milhões de dígitos (**P** é também um número primo). A fundação estabeleceu o prêmio para promover a computação cooperativa que usa a Web.

- Em 23 de agosto de 2008, matemáticos de UCLA encontram o 45º número primo de **Mersenne**, $2^{43\ 112\ 609}-1$. Número enorme com **12 978 189** de dígitos. O número foi encontrado usando uma rede de 75 computadores que rodam Windows XP.

- Em 6 de setembro de 2008, Hans-Michael Elvenich na Alemanha encontrou o 46º número primo de **Mersenne**, $2^{37\ 156\ 667}-1$ com **11 185 272** de dígitos.

- Ambos primos foram verificados independentemente por vários pesquisadores (USA, New Zealand, França, Canadá e Espanha) que usaram diferentes arquiteturas de computadores e algoritmos. As verificações demoraram entre 5 e 13 dias.

Vamos logo ao prêmio.

- Em 12 de abril de 2009, Odd Magnar Strindmo da Noruega encontrou o 47º número primo de **Mersenne**, $2^{42\,643\,801}-1$. Outro número enorme com **12 837 064** de dígitos.

- Desde 1996 milhares de pessoas do mundo todo tem participado do **GIMPS - Great Internet Mersenne Prime Search**, sistema cooperativo que une esforços para encontrar números de **Mersenne** pela Internet. Em 4 de setembro de 2006 foi encontrado o 44º número de **Mersenne**, $2^{32\,582\,657}-1$ com **9 808 358** dígitos. Dígitos insuficientes para reclamar pelo premio da EFF.

- Existem outros prêmios da EFF para o primeiro que descobrir um número primo com pelo menos:

- 1.000.000 de dígitos. Valor **$50.000,00** (Entregue 6 de abril de 2000).
- 10.000.000 de dígitos. Valor **$100.000,00** (Por ser entregue).
- 100.000.000 de dígitos. Valor **$150.000,00**.
- 1.000.000.000 de dígitos. Valor **$250.000,00**.

- **http://www.eff.org/**

Como posso participar?

- **Qualquer individuo pode participar. É necessário se inscrever no site da A Electronic Frontier Foundation (EFF) oferecia um prêmio de US$ 100.000,00 para o primeiro que conseguisse encontrar um número primo de Mersenne (2^p-1) com mais de 10 milhões de dígitos (P é também um número primo). A fundação estabeleceu o prêmio para promover a computação cooperativa que usa a Web.**

- **Em 23 de agosto de 2008, matemáticos de UCLA encontram o 45º número primo de Mersenne, $2^{43\ 112\ 609}-1$. Número enorme com 12 978 189 de dígitos. O número foi encontrado usando uma rede de 75 computadores que rodam Windows XP.**

- **Em 6 de setembro de 2008, Hans-Michael Elvenich na Alemanha encontrou o 46º número primo de Mersenne, $2^{37\ 156\ 667}-1$ com 11 185 272 de dígitos.**

- **Ambos primos foram verificados independentemente por vários pesquisadores (USA, New Zealand, França, Canadá e Espanha) que**

Resumo:

A teoria dos números tem como objeto de estudo as propriedades de todos os números e conforma um dos ramos mais vasto e fascinante da matemática.

As questões referentes aos números primos formam a essência da teoria dos números. Frequentemente, ao estudar os números primos nos defrontamos com problemas aparentemente elementares que acabam se mostrando difíceis de serem resolvidos e até misteriosos.

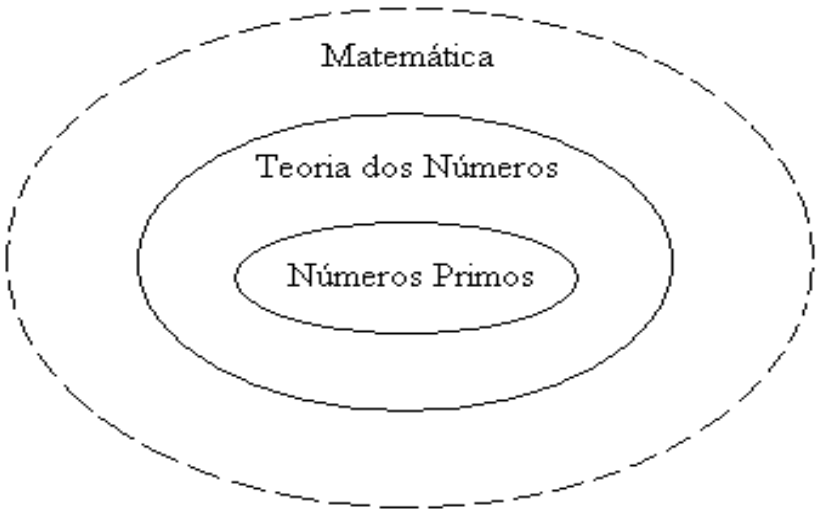
Aqui abordaremos algumas questões sobre os números primos.

- Quantos números primos existem?
- Existem fórmulas que geram os primos?
- Como saber se um inteiro é primo?
- Como são distribuídos os primos num dado intervalo de números inteiros?
- Abordaremos brevemente algumas conjeturas clássicas e problemas em aberto.
- Mencionaremos alguns exemplos onde todo este conhecimento teórico é usado em problemas práticos.

TEORIA DOS NÚMEROS

Campo vasto e fascinante da matemática (Aritmética Superior) que estuda as propriedades de todos os números.

A grande dificuldade em provar resultados "*simples*" na teoria dos números levou Gauss (*príncipe das matemáticas*), que chamava a matemática de *rainha das ciências*, chamar a teoria dos números de *rainha da matemática* (Beiler 1966, Goldman 1997).



Números Primos e fatoração em primos são essenciais na teoria dos números

Entre todos os tópicos que compõem a teoria dos números apenas falaremos sobre os números primos.

SOBRE OS NÚMEROS PRIMOS

- **Pequena introdução sobre os números primos.**
- **Questões básicas como:**

  - Quantos números primos existem?

  - Existem funções (fórmulas) que geram os primos?

  - Como saber se um inteiro é primo?

  - A distribuição dos primos num dado intervalo de números inteiros?
- **Algumas hipóteses, conjeturas clássicas e problemas abertos.**
- **Uma aplicação.**
- **Comentários finais.**
- **Referências.**

Pequena introdução sobre os números primos.

- Definição: O número natural N>1 é chamado primo (P) se seus únicos divisores (sem deixar resto) são 1 e ele próprio. Caso contrário é chamado composto e pode ser decomposto como o produto de primos.

$$N = P_1^{k_1} \cdot P_2^{k_2} \cdots P_n^{k_n}$$

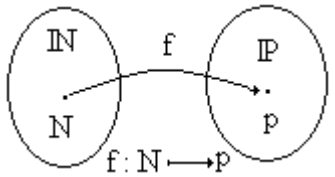
(Chamado Fatoração - Algoritmo de Fatoração – Algoritmos Eficientes=Grande Desafio).

Exemplo: 13 é primo e $24=2^3{}_*3$ é composto.

- Exceto o 2 todos os números primos são impares.
- Teorema Fundamental da Aritmética: Todo inteiro positivo (N≠1) é produto de números primos, de maneira única a menos da ordem dos fatores.
- A palavra "Primo" vem do Latim "Primus" que significa primeiro ou mais importante. Há milênios os Gregos já sabiam que os primos são os objetos mais importantes da matemática porque são os tijolos que constroem todos os números. Ou seja, são os átomos da aritmética. O DNA da aritmética.
- O número 1 é um caso especial. As vezes não é considerado nem primo nem composto (*Wells 1986, p. 31*). Outras, considerado o primeiro primo (*Goldbach 1742; Lehmer 1909; Lehmer 1914; Hardy and Wright 1979, p. 11; Gardner 1984, pp. 86-87; Sloane and Plouffe 1995, p. 33; Hardy 1999, p. 46*). Se 1 for considerado primo deveria ser mudado alguns enunciados de teoremas. Mas como é uma questão de definição não é discutível (*Tietze 1965, p. 2, Derbyshire 2004, p. 33*) e por acordo o 1 não é considerado primo.

Q. B. 1: Quantos números primos existem?

- A resposta não é intuitivamente simples. Temos certeza de uma coisa. O conjunto dos primos pode ser apenas uma e só uma das seguintes possibilidades: finito ou infinito.
- Note que os naturais se classificam em pares e impares.
- Como todos os pares são múltiplos de 2, só o 2 é primo e o outros pares não.
- Um raciocínio parecido poderia ser feito para os impares.
- Será que existe um número finito de impares que geram todos os outros impares como acontece com os pares? A resposta é não. Portanto, o conjunto dos números primos é infinito.
- Como mostrar que um conjunto tem infinitos elementos?
- Se conhecem dois métodos.
- 1 – Método direto: estabelece uma correspondência injetora entre um conjunto infinito conhecido e o conjunto em estudo.



- 2 – Método indireto: mostra que é impossível que o conjunto seja finito, logo tem que ser infinito. Isto pode ser feito através de uma contradição ou absurdo.

Q. B. 1: Quantos números primos existem?

- Teorema (2º de Euclides): O conjunto dos números primos é infinito.
- Definição: A função $\pi(N)$, $\pi : \mathrm{IN} \to \mathrm{IN}$ se define como a quantidade de primos que existem no intervalo $[2, N]$.
- Teorema (2º de Euclides outra versão): $\lim_{N \to \infty} \pi(N) = +\infty$.
- Existem varias demonstrações para a afirmação de Euclides:

1 - Proposição IX.20 dos ***Elementos*** de Euclides (Tietze 1965, pp. 7-9).

2 - A demonstração de Euler foi decisiva para os avanços futuros. Sem ela seria difícil ter se chegado à função Zeta de Riemann e a famosa hipótese de Riemann.

3 - Existem muitas outras demonstrações. Todas baseadas no método indireto. Quando existir a primeira demonstração baseada no método direto teremos a primeira boa formula para encontrar números primos.

Q. B. 1: Quantos números primos existem?

Demonstração de Euclides (Prova pelo absurdo ou contradição, método indireto)

Suponha o contrário da afirmação do teorema, ou seja, o conjunto dos números primos é finito e eles são $P_1, P_2, \cdots, P_m$. Considere o número $N = P_1 \cdot P_2 \cdots P_m + 1$.

Existem duas alternativas:

1) N é primo e como $N > P_i \ (i = 1, ..., m)$ encontramos um novo primo. O que é uma contradição.

2) N é composto e por definição tem um fator primo $q < N$

$N = q \cdot M = P_1 \cdot P_2 \cdots P_m + 1$. Como por hipótese o conjunto dos primos é finito, q deveria ser um dos P_i , logo divide $P_1 \cdot P_2 \cdots P_m = N - 1$. Se q divide N e $N - 1$, então divide $N - (N - 1) = 1$. Isto é um absurdo.

Portanto, o conjunto de números primos não é finito.

Q. B. 1: Quantos números primos existem?

Demonstração de Euler (Prova pelo absurdo ou contradição, método indireto)

Suponha o contrário da afirmação do teorema, ou seja, o conjunto dos números primos é finito e eles são $P_1, P_2, \cdots, P_m$. Considere o número definido pelo produto de *m* séries geométricas. São séries convergentes com soma $\left(1 - 1/P_i\right)^{-1} = \frac{P_i}{(P_i - 1)}, \; i = 1, \ldots, m$.

$$\tilde{P} = \left(\sum_{n=0}^{\infty} \frac{1}{P_1^{\,n}}\right) \cdot \left(\sum_{n=0}^{\infty} \frac{1}{P_2^{\,n}}\right) \cdots \left(\sum_{n=0}^{\infty} \frac{1}{P_m^{\,n}}\right) = \frac{P_1}{(P_1 - 1)} \cdot \frac{P_2}{(P_2 - 1)} \cdots \frac{P_m}{(P_m - 1)}$$

Logo podemos expandir $\tilde{P}$ e obtemos

$$\tilde{P} = \left(1 + \frac{1}{P_1} + \frac{1}{P_1^2} + \frac{1}{P_1^3} + \cdots\right) \cdot \left(1 + \frac{1}{P_2} + \frac{1}{P_2^2} + \frac{1}{P_2^3} + \cdots\right) \cdots \left(1 + \frac{1}{P_m} + \frac{1}{P_m^2} + \frac{1}{P_m^3} + \cdots\right) = \sum_{n_1, \cdots, n_m = 0}^{\infty} \frac{1}{P_1^{n_1} P_2^{n_2} \cdots P_m^{n_m}}$$

Pelo teorema fundamental da aritmética todo inteiro positivo é representado unicamente como $N = P_1^{n_1} \cdot P_2^{n_2} \cdots P_m^{n_m}$. Logo temos

$$\tilde{P} = \sum_{n_1, \cdots, n_m = 0}^{\infty} \frac{1}{P_1^{\,n_1} P_2^{\,n_2} \cdots P_m^{\,n_m}} = \sum_{N=1}^{\infty} \frac{1}{N} = \infty$$

que é a série harmônica. Novamente chegamos a um absurdo. O número finito $\tilde{P}$ não pode ser infinito. Então o conjunto dos primos não pode ser finito.

Q. B. 2: Existem funções que geram os primos?

- Os números naturais podem ser classificados em impares e pares. E mais, temos uma formula para saber quando um natural *N* arbitrário é par *N=2M* ou impar *N=2M+1*, onde *M* é outro natural.

- O mesmo não pode ser dito para o caso dos números primos e compostos. Não existe uma função que gere todos os números primos, nem também um algoritmo eficiente do tipo P - Polinomial que encontre os fatores de qualquer número natural composto.

- A odisséia pela busca de formulas (funções) que gerem primos pode ser dividida em três níveis:

1- A formula de ouro que prediga todos os primos em ordem e nenhum falso primo.

2- A formula que prediga uma infinidade de primos, mas não todos, e nenhum falso primo.

3- A formula que prediga falsos primos e nenhum primo. Ou a formula que descreva o conjunto dos primos através de funções mais simples (polinômios).

- Se alguém descobrir qualquer uma destas três possíveis formulas se tornará famoso no mundo da matemática e da ciência.

- Como este tema faz parte dos fundamentos da matemática (aritmética) todos nós estamos quase que em igualdade de condições para participar da corrida. Pode ser que este alguém seja um aluno do Ensino Fundamental e/ou Médio. Por que não?

Q. B. 2: Existem funções que geram os primos?

- No século III AC surgiu o primeiro método para gerar primos. Conhecido como *Crivo de Erastóstenes* e consiste em:

1- escrever todos os números naturais até *N*.

2- riscar, em seqüência, todos os múltiplos de 2, 3, 5, ..., de cada primo $P < \sqrt{N}$. Isto é feito localizando o primeiro múltiplo *P* e riscando este e cada *P* -ésimo número seguinte.

3- O que restar serão todos primos.

Este método é recursivo porque para saber se *N* é primo devemos conhecer todos os primos $P < \sqrt{N}$. O método não fornece os fatores primos de um número composto. Além disto, o método é muito lento quando *N* é grande, mesmo até para computadores sofisticados. O algoritmo deste método é classificado como algoritmo Não Polinomial NP.

- Encontrar padrões nos primos tem atraído matemáticos por mais de 2000 anos. Muitos morreram tentando desvendar enigmas dos primos. Outros apostaram toda sua careira profissional em conjeturas sem sucesso algum.

Q. B. 2: Existem funções que geram os primos?

- Odisséia 1: Encontrar uma função f tal que $\forall N \; f(N) = P_N$, onde P_N é o N - ésimo número primo. Ou seja, a função que gera todos os primos em ordem.

Um exemplo pouco útil: $P_N = 1 + \sum_{M=1}^{2^N} \left[\sqrt[N]{\frac{N}{1+\pi(M)}} \right]$, onde $[X]$ é a parte inteira de X.

Obtida por Willans em 1964 é uma formula miraculosa, bonita e inútil. Note que, por exemplo, para conhecer o décimo primo devemos contar quantos primos existem até 1024.

$$29 = P_{10} = 1 + \sum_{M=1}^{1024} \left[\sqrt[10]{\frac{10}{1+\pi(M)}} \right]$$

Existem muitos outros exemplos que se encaixam na Odisséia 1.

Vamos agora para outro nível de Odisséia, a Odisséia 2.

Q. B. 2: Existem funções que geram os primos?

- Odisséia 2: Encontrar uma função f tal que $\forall N \quad f(N)$ é primo e se $N \neq M$ então $f(N) \neq f(M)$. Ou seja, encontrar uma infinidade de primos, mas não todos e nem em ordem.

Um exemplo pouco útil: $f(N) = \left[2^{2^{2^{\cdot^{\cdot^{\cdot^{2^w}}}}}} \right]$, onde $[X]$ é a parte inteira de X , $2^{2^{2^{\cdot^{\cdot^{\cdot^{2^w}}}}}}$ representa *N* etapas de expoentes e $w = 1{,}92827800 \ldots$.

Obtida por Wright em 1954. A formula apresenta um defeito grave. Foi demonstrada a existência de *w*, mas seu cálculo é feito com certa aproximação. Se não conhecemos bem os decimais de *w* temos erros, a formula falha e obtemos números que não são primos.

Existem muitos outros exemplos que se encaixam na Odisséia 2.

Vamos agora para outro nível de Odisséia, a Odisséia 3.

Q. B. 2: Existem funções que geram os primos?

- Odisséia 3: Encontrar polinômios de uma ou varias variáveis que descrevam o conjunto dos números primos.

  Para polinômios de uma variável existe um teorema que garante que não é possível gerar todos os primos. Entretanto, podemos gerar com este tipo de polinômios números primos dando valores inteiros sucessivos a variável a partir de zero.

  Um bom exemplo devido a Euler: $f(X) = X^2 + X + 41, \quad \forall N = 0,1,2,...,39$

  $f(N)$ é primo, mas para *N=40* temos $f(40) = 40(40+1)+41 = 41 \cdot 41$

  Conjetura de Schinzel e Zierpinski: Será que para todo polinômio *f(x)* com coeficientes inteiros e com mdc igual a 1, de grau maior ou igual a 1, existe um número natural *N* tal que *f(N)* seja primo?

  Em 1970 Matijasevic resolveu pela negativa o décimo problema de Hilbert. Seu trabalho permite demonstrar um resultado surpreendente:

  Existe um polinômio de grau 25 com 26 variáveis tal que quando atribuímos valores inteiros positivos as variáveis se obtém inteiros que quando são positivos são também primos e assim obtemos todos os primos. Ou em outras palavras, o conjunto dos primos é o conjunto dos valores positivos de um polinômio de grau 25 com 26 variáveis.

Q. B. 2: Alguns tipos de primos.

- Muitos pensadores achavam que números da forma 2^P-1 fossem primos para todos os primos P.

- Em 1536 Hudalricus Regius mostrou que $2^{11}-1 = 2047=23x89$ não era primo.
- Por volta de 1603 Pietro Cataldi verificou que $2^{17}-1$ e $2^{19}-1$ eram primos, mas declarou incorretamente que 2^P-1 fosse primo para P=23, 29, 31 e 37.
- Em 1640 Fermat mostrou que Cataldi estava errado para 23 e 37.
- Em 1644 o monge francês **Marin Mersenne** (1588-1648) declarou no prefacio da obra *Cogitata Physica-Mathematica* que os números 2^P-1 eram primos para P=2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 e composto para todos os outros inteiros positivos N < 257. Esta conjetura estava errada, mas seu nome ficou ligado para sempre a estes números.
- Era óbvio para os colegas de Mersenne que ele não tinha testado todos estes números, mas eles também não puderam verificar isto.
- Em 1738 Euler mostrou que Cataldi estava errado para 29 e em 1750 que Regius, Cataldi e Mersenne estavam certo para 31.
- Em 1876, depois de um século, Lucas verificou que $2^{127}-1$ também era primo.
- Em 1883 Pervouchine mostrou que $2^{61}-1$ era primo, logo Mersenne tinha errado.
- A inícios do século XX Powers mostrou que Mersenne esqueceu de dois primos $2^{89}-1$ e $2^{107}-1$.

- Em 1947 a lista de Mersenne foi verificada por completo e determinado que a lista correta para $P \leq 258$ é: N=2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127.

Q. B. 2: Alguns tipos de primos.

- Primos de Mersenne: São primos da forma 2^P-1, onde P também é primo. Hoje se conhecem apenas 47 primos de Mersenne.


Pierre de Fermat

N	$2^{2^N}+1$	Primo
0	3	Sim
1	5	Sim
2	17	Sim
3	257	Sim
4	65537	Sim
5	6700417x641	Não

- Primos de Fermat: Em 1640 Fermat conjeturou que números da forma $2^{2^N}+1$ eram primos para *N=0, 1, 2, ...* Números deste tipo quando são primos são chamados primos de Fermat. Os cinco primeiros elementos desta seqüência são primos. Em 1732 Euler descobriu que *F(N=5)* era composto. Mais ainda, mostrou que todo divisor de *F(N)* para *N>2* tem a forma $K \cdot 2^{(2+N)}+1$. Para *N=5* temos *128K+1*. Este resultado de Euler é a base do teste de Pepin para saber se um número de Fermat é primo.

- Primos Gêmeos: São primos da forma {*P,P+2*}. Exemplos, {3,5}, {5,7}, {11,13}.

Q. B. 3: Como saber se um inteiro é primo?

- Dado um natural arbitrário *N* temos como saber se é primo efetuando um número finito de operações?

- O *Crivo de Erastóstenes* é o método mais antigo conhecido. Apenas devemos dividir *N* por todo número primo *P* tal que $P^2<N$. O grande problema deste método é que o número de operações se torna muito grande quando *N* cresce.

- **O Desafio:** Encontrar um algoritmo *A*, cujo número de operações efetuadas sobre os algarimos de *N* permaneça limitado por uma função f_A que não cresça rapidamente com *N*. Ou seja, $f_A(N)$ é limitado por um polinômio no número de algarismos $1+[\log N]$ de *N*.

  Em outras palavras, o tempo de processamento não cresce exponencialmente (tempo polinomial) em relação ao tamanho de *N*. Algoritmos deste tipo são chamados Polinomiais P, caso contrário são chamados Algoritmos Não Polinomiais NP.

- Este problema ficou em aberto durante séculos até 2003, quando o Prof. Manindra Agrawal e seus dois alunos de doutorado Neeraj Kayal e Nitin Saxena (Depto. de CC do Instituto Indiano de Tecnologia em Kanpur) provaram que os primos estão em P. O algoritmo criado por eles AKS decide em tempo polinomial, sem margem de erro, se um número *N* é primo, mas se for composto não permite encontrar os fatores primos.

- Já existia um algoritmo polinomial, mas era probabilístico. A resposta dos algoritmos probabilísticos sempre tem uma pequena margem de erro.

Q. B. 3: Como saber se um inteiro é primo?

- Existem vários tipos de algoritmos que podem ser classificados como:
  - para números arbitrários –- de forma especial,
  - justificados –- baseados em conjeturas,
  - deterministas –- probabilísticos.

- Alguns exemplos:

- 1. Algoritmo de Miller (1975) baseado na hipótese generalizada de Riemann. Algoritmo determinista, não justificado, para números arbitrários a tempo polinomial. $f_A(N) \leq c(\log N)^5$

- 2. Algoritmo de Adleman, Pomerance e Rumely (1983). Algoritmo determinista, justificado, para números arbitrários a tempo não polinomial (quase polinomial). $f_A(N) \leq (\log N)^{c \log(\log(\log N))}$

- 3. Algoritmo de Baillie e Wagsiaff, Rabin e outros são probabilísticos. Quando aplicamos o algoritmo ao número N obtemos que N é composto ou que é primo com grande probabilidade.

- 4. Algoritmos que se aplicam a números da forma N±1, onde todos ou muitos dos fatores primos de N são conhecidos. Teste para números N+1 são baseados no pequeno teorema de Fermat (Pepin, 1877, para números de Fermat $2^{2^N}+1$). Teste para números N-1 utilizam as seqüências de Lucas, 1878, números de Mersenne 2^P-1.

Q. B. 4: A distribuição dos primos num dado intervalo de números inteiros?

- No século XIX Beltrand observou que para $N > 1$ no intervalo $[N, 2N]$ existe pelo menos um primo.
- Chebyshev fez uma demonstração rigorosa desta observação. Isto permite encontrar números primos num intervalo desejado do tipo $[N, 2N]$.
- Gauss descobriu que para N grandes $\pi(N) \sim \dfrac{N}{\log N}$.
- Depois Chebyshev mostrou que se N é grande, então

$$0{,}9\frac{N}{\log N} < \pi(N) < 1{,}1\frac{N}{\log N}$$

- Quase um século depois da descoberta de Gauss, Hadamard e De La Vallée Poussin demonstraram a afirmação que hoje se conhece como o **Teorema do Número Primo**.

$$\lim_{N\to\infty} \frac{\pi(N)}{\dfrac{N}{\log N}} = 1 \quad \text{ou} \quad \lim_{N\to\infty} \frac{\left|\pi(N) - \dfrac{N}{\log N}\right|}{\pi(N)} = 0$$

Observe que isto pode ser interpretado como um erro relativo.

Hipóteses, conjeturas e problemas abertos.

1- Não se conhece um algoritmo eficiente que fatore um inteiro arbitrário, mas não foi provado que não exista tal algoritmo.

2- Não se sabe se existe um número infinito de primos da forma N^2+1 (Hardy e Wright 1979, pág. 19; Ribenboim 1996, pp. 206-208).

3- Não se sabe se existe um número infinito de primos gêmeos (Conjetura dos Primos Gêmeos).

4- Não se sabe se existe sempre um primo entre N^2 e $(N+1)^2$ (Hardy e Wright 1979, pág. 415; Ribenboim 1996, pp. 397-398).

Os itens 3 e 4 são dois dos problemas de Landau (Matemático famoso de personalidade introvertida).

5- Conjetura de Schinzel e Zierpinski: Será que para todo polinômio f(x) com coeficientes inteiros e com mdc igual a 1, de grau maior ou igual a 1, existe um número natural N tal que f(N) seja primo?

Hipóteses, conjeturas e problemas abertos.

6- Conjetura de Goldbach: Todo número par N>2 é a soma de dois primos.

Verifying the Goldbach Conjeture up tp 4 10^{14} , Math. Comp., 70 (2001), 1745-1749.

8- O conjunto dos primos de Fermat é finito?

9- Hipótese de Riemann: Todos os zeros não triviais da função Zeta de Riemann estão na linha reta do plano complexo Re(s) = 1/2.

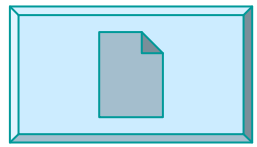
$$\zeta(s)=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\cdots+\frac{1}{n^s}+\cdots=\sum_{n=1}^{\infty}\frac{1}{n^s}$$

Se $s=1$ é a série harmonica (divergente $\forall s\le 1$). Para $s>1$a série converge. Considerando que todo número composto pode ser fatorado em primos temos os produtos de Euler

$$\zeta(s)=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\cdots+\frac{1}{n^s}+\cdots=\left(1+\frac{1}{2^s}+\frac{1}{4^s}+\cdots\right)\cdot\left(1+\frac{1}{3^s}+\frac{1}{9^s}+\cdots\right)\cdots\left(1+\frac{1}{p^s}+\frac{1}{\left(p^2\right)^s}+\cdots\right)\cdots$$

Note que de um lado aparece a função Zeta e do outro os números primos

$$\zeta\left(s\right)=\left(\sum_{n=0}^{\infty}\frac{1}{\left(P_1{}^n\right)^s}\right)\cdot\left(\sum_{n=0}^{\infty}\frac{1}{\left(P_2{}^n\right)^s}\right)\cdots\left(\sum_{n=0}^{\infty}\frac{1}{\left(P_m{}^n\right)^s}\right)\cdots$$



Hipóteses, conjeturas e problemas abertos.

- Números perfeitos: São os naturais que coincidem com a soma de seus divisores.

- Muitas culturas antigas atribuíam a estes números um significado religioso e mágico especial.

Por exemplo os três primeiros números perfeitos são:

$6 = 1 + 2 + 3,$

$28 = 1 + 2 + 4 + 7 + 14,$

$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248.$

- Um cristão antigo explicou que DEUS poderia ter criado o mundo em um instante, mas escolho um número perfeito para isto 6.

- Os judeus antigos diziam que a perfeição do universo foi mostrada pelo período da lua de 28 dias.

- Teorema: Se 2^k-1 é primo, então $2^{k-1}x(2^k-1)$ é perfeito e todo número perfeito par tem esta forma.

10- Não se sabe se existem números perfeitos impares. Se houver eles devem ser grandes, pelo menos 300 dígitos, e devem ter muitos fatores primos.

Uma aplicação.

- Muitos podem achar que encontrar primos de Mersenne é uma tarefa sem graça e ridícula, mas números primos e a difícil tarefa de fatorar números compostos em primos é parte do sistema que permite a transferência "segura", através de códigos numéricos, de trilhões de dólares ao redor do mundo.

- Se alguém inventar um método geral e eficiente para fatorar números inteiros tornará inúteis a maioria dos esquemas de criptografia que são usados hoje por bancos e instituições governamentais.

- Devido ao papel importante dos primos nos algoritmos de criptografia, por exemplo RSA, eles podem se tornar commodities comerciais de grande valor. Já existe uma patente americana: *Schlafly, R. "Partial Modular Reduction Method." United States Patent . December 13, 1994*.

- O que é Criptografia?

Uma aplicação.

Criptografia?

Estuda como codificar informação que só pode ser decodificada pelo receptor, embora outros possam ter acesso a informação codificada.

Para codificar se usa uma chave secreta e para decodificar a informação, tradicionalmente, o receptor aplica a chave ao contrário. Portanto, a chave é o ponto fraco do sistema de segurança. Tanto o emissor como o receptor devem conhecer a chave ou parte dela.

- Em 1970 Whitfield Diffie e Martin Hellman se perguntaram se existiria algum processo matemático fácil de ser realizado em um sentido e difícil de ser feito na direção oposta.
- Tal processo seria uma chave ótima porque poderia dividir a chave em duas partes sem relação: uma parte codificadora de domínio público e outra decodificadora sob domínio restrito.
- Em 1987 Ronald Rivest, Adi Shamir e Leonard Adleman (matemáticos e cientistas da computação do MIT) perceberam que o processo de fatorar números compostos em primos seria uma boa escolha. Para construir a parte decodificadora da chave usaria dois números primos enormes (80 dígitos cada). A parte codificadora da chave é formada pelo número composto produto dos dois primos.

Comentários finais

- Física quântica e números primos estão indissoluvelmente relacionados.

  O físico Freeman Dyson em seu artigo "*Oportunidades Perdidas*" de 1972 descreve como a relatividade poderia ter sido descoberta 40 anos antes de Einstein se os matemáticos (em Göttingen ou outros) tivessem falado com físicos da época (concentrados nas equações de Maxwell). Os ingredientes estavam lá em 1865.

  Freeman Dyson e o teórico dos números Hugh Montgomery tiveram a chance de trocar idéias no Instituto de Estudos Avançados de Princenton. Eles descobriram que *os zeros da linha crítica de Riemann e os níveis de energia do núcleo de um átomo grande como Érbio tem padrões semelhantes*.

  Se pudéssemos entender a matemática que descreve a estrutura do núcleo atômico, talvez a mesma matemática poderia resolver a Hipótese de Riemann.

- Pergunta intrigava biólogos sobre as Cigarras.

Comentários finais

- Pergunta intrigava biólogos sobre as Cigarras.

As cigarras possuem o ciclo de vida (Nc) mais longo entre os insetos. A vida delas começa embaixo da terra, onde sugam o suco da raiz das árvores. Depois de 17 anos (*Magicicada Septendecim*) as cigarras adultas emergem do solo e se espalham pelo campo. Depois de algumas semanas se acasalam, põem seus ovos e morrem. Outra espécie, a *Magicicada Tredecim* tem seu ciclo de vida a cada 13 anos.

Por que o ciclo de vida das cigarra é tão longo?

Por que seus ciclos de vida são números primos?

Será que um ciclo de vida correspondente a um número primo de anos oferece vantagem evolutiva?

Nc - ciclo de vida da cigarra
Np - ciclo de vida do parasita
Ne – período em que coincide a reprodução da cigarra e o parasita

Comentários finais

- Pergunta intrigava biólogos sobre as Cigarras.

  Uma teoria sugere que a cigarra tem um parasita com ciclo de vida longo (Np) que ela tenta evitar. Para que a aparição da cigarra e o parasita não coincida com muita freqüência Nc≠MxNp. Logo, para evitar se encontrar (Ne) com seu parasita a melhor estratégia da cigarra seria ter um ciclo longo que fosse primo. Neste caso Ne=NcxNp e o parasita tem apenas duas boas escolhas de ciclo de vida para aumentar a freqüência de coincidências: Np=1 ou Np=Nc. Porém, se tiver Np=1 é pouco provável que o parasita sobreviva porque durante Nc-1 anos não encontrará a cigarra para parasitar. Por outro lado, se quiser ter Np=Nc as gerações de parasitas terão que evoluir e passar pelo ciclo Nc-1, o que significa que durante um período da evolução do parasita sua reprodução coincidirá com as cigarras a cada Ne=Ncx(Nc-1)=17x16=272 anos. Em ambas possibilidades Np=1 ou Np=Nc o ciclo longo de vida das cigarras as protege do parasita. Isto pode explicar porque o suposto parasita nunca foi encontrado e o ciclo de vida tão longo das cigarras.

- Albert Einstein costumava dizer, "*Se o universo (e tudo nele) for um produto de aleatoriedades, ciência seria impossível*." A relação causa-efeito é a base do método científico.

Boas Referências na Internet

- Se procurarmos por: *mathematical world* no Google aparecem mais de 34.300.000 registros. Se refinamos a busca por: *primes* aparecem mais de 79.100 registros.

- Alguns SITES interessantes sobre números primos:

http://primes.utm.edu/

http://www.asthe.org/chongo/tech/math/prime/prime_press.html

http://mathworld.wolfram.com/

http://www.claymath.org/

http://www.claymath.org/public_lectures/

http://mathtourist.blogspot.com/2008/08/new-formula-for-generating-primes.html

http://www.ams.org/ams/mathnews/prime.html

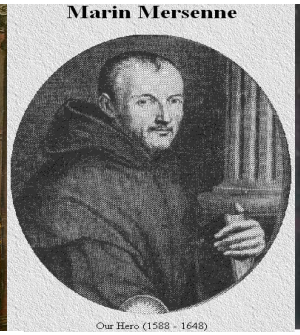
http://www.mersenne.org/

http://www.cite-sciences.fr/francais/ala_cite/science_actualites/sitesactu/question_actu.php?langue=an&id_article=4283

Bons livros e artigos de Referências

- O último teorema de Fermat, Simon Singh, 2001, Editora Record.
- Tio Petros e a Conjetura de Goldbach, Apostolos Doxiadis, 2001, Editora 34 Ltda.
- A música dos números primos, Marcus du Sautoy, 2008, Zahar.
- Vendendo primos, Paulo Ribenboim, Matemática Universitária No 22/23, junho/dezembro de 1997.
- Existem funções que geram os números primos?, Paulo Ribenboim, Matemática Universitária No 15, dezembro de 1993.
- Os recordes dos números primos, Paulo Ribenboim, Matemática Universitária No 14, dezembro de 1992.
- A distribuição dos números primos, José Felipe Voloch, Matemática Universitária No 6, dezembro de 1987.
- Introdución a la teoría analítica de números, T. M. Apostol, Editora Reverté S.A., 1980.

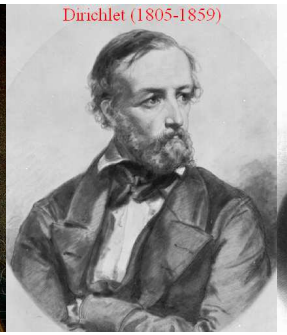

Euclides (360-295 AC)

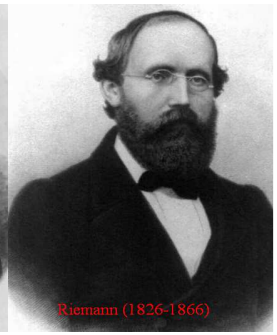


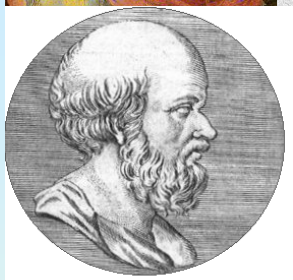
Our Hero (1588 - 1648)


Pierre de Fermat


Euler (1707-1783)






Eratóstenes (276 - 194 a.C.)

MUITO OBRIGADO!

Espero que o tema tenha sido interessante e que o apresentador tenha feito um bom trabalho.

Pelos menos que tenha satisfeito as expectativas de alguns.

E que de alguma forma tenha compensado parte do esforço da Comissão Organizadora do evento.

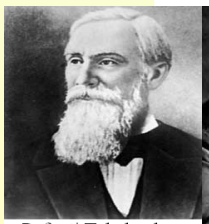

Hadamard (1865-1963)


Hilbert (1862-1943)


Charles Jean de la Vallée-Poussin (1866-1962)

Agradecimentos Especiais

- Ao Prof. Nirzi Andrade pelo apoio recebido.
- A Coordenação do Evento.
- A todos os presentes.


Pafnuti Tchebychev (1821-1894)


Landau (1877-1938)


Godfrey Harold) Hardy


Gödel

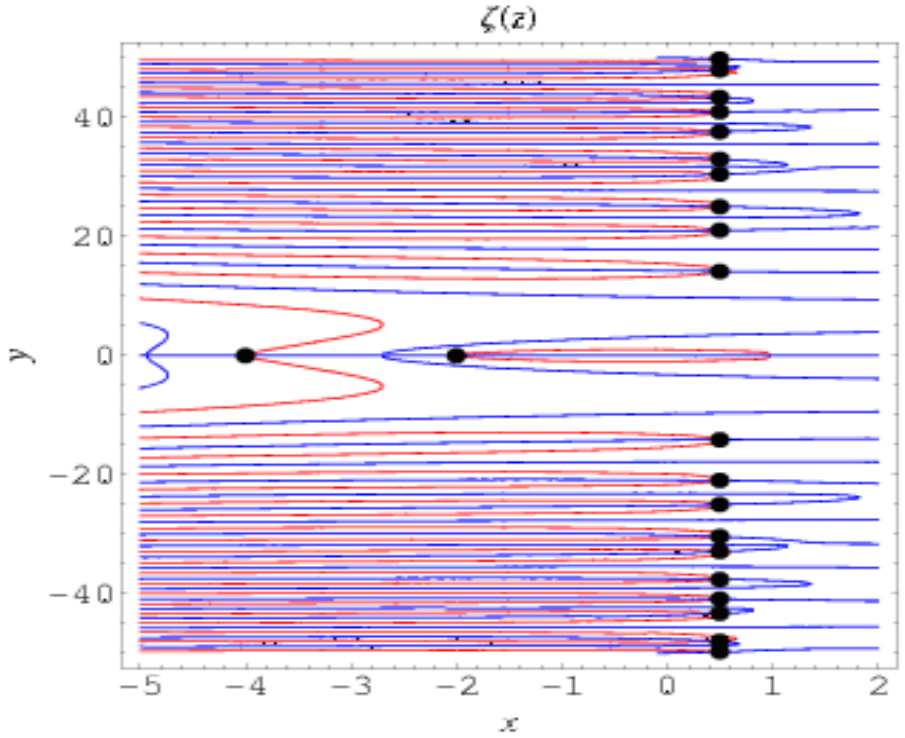

Freeman Dyson


H. Montgomery

Hipótese de Riemann.

- A função **Zeta de Riemann** estabelece uma ponte entre os primos e o mundo de geometria. Explorando os zeros da função Zeta encontramos informação crucial sobre a natureza dos primos. Riemann transformou primos em pontos onde a função Zeta tem seus zeros não triviais. Quando ele encontrou os 10 primeiros zeros da função apareceu um padrão surpreendente. Os zeros não se espalharam por toda parte. Parecia que os zeros não triviais se localizavam em uma linha reta. Ele não acreditava que isto fosse uma coincidência e conjeturou o que hoje é conhecido como **Hipótese de Riemann**.

  - Os zeros triviais são alcançados em s=-2, -4, -6, ... (todos os inteiros pares negativos). Os zeros não triviais são alcançados dentro de uma faixa crítica definida por s=a+ib, onde 0<a<1 e determinados valores de b.



parte —— real —— imaginaria