Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Departamento de Matemática

Números Primos

Ary Camargo Rizel

Belo Horizonte
2014

Ary Camargo Rizel

NÚMEROS PRIMOS

Monografia apresentada ao Departamento de Matemática do Instituto de Ciências Exatas (ICEX) da Universidade Federal de Minas Gerais. Requisito parcial à obtenção do título de especialização Latu Senso para professores com ênfase em cálculo.

Orientação: Prof. Dr. André Gimenez Bueno.

Belo Horizonte
Novembro - 2014

FOLHA DE APROVAÇÃO

Data de apresentação: 28/11/2014.

Banca examinadora:

_____
Prof. Dr. André Gimenez Bueno

_____
Prof. Dr. Paulo Antônio Fonseca Machado

_____
Prof. Dr. Vitor Bekkert

AGRADECIMENTOS

À Deus, por me conceder força para vencer mais uma etapa em minha vida.

À minha esposa Lucinha, pelo apoio, carinho, compreensão e principalmente por me aceitar como eu sou.

Ao professor André Gimenez Bueno meu orientador pelo incentivo, disponibilidade, atenção e apoio durante todo o percurso.

Em especial a professora Maria Imaculada Marcenes minha primeira orientadora em trabalhos de monografia pelo grande aprendizado durante sua orientação que guardo comigo até hoje e me auxiliaram na elaboração deste.

Enfim, a todos aqueles que contribuíram para a realização deste trabalho.

Muito Obrigado.

RESUMO

Este trabalho tem como objetivo apresentar um pequeno resumo sobre os números primos. Assunto que vem atraindo muitos matemáticos eminentes desde o princípio, e ainda hoje nos apresenta muitos desafios. Iniciaremos com os conceitos mais fundamentais sobre o tema. Em seguida, apresentaremos algumas demonstrações clássicas da infinidade de números primos. Abordaremos os principais teoremas que nos permitem reconhecer um número primo e faremos um pequeno relato histórico dos estudos sobre a distribuição de números primos. Citaremos algumas funções que geram números primos. E por fim, teceremos alguns comentários a respeito de casos particulares de primos que foram estudados.

Palavras Chaves: Teoria dos números, Números naturais, Números primos.

ABSTRACT

This work aims to present a short summary about prime numbers. This subject has attracted many outstanding mathematicians from the early days on, and still presents many challenges. We begin with the most fundamental concepts of the subject. Next, we present some classical proofs of the infinity of primes. Some primality tests will be discussed, and also the distribution of prime numbers. Finally, we will quote some functions that generate prime numbers.

Key Words: Theory of numbers, Natural numbers, Prime numbers.

SUMÁRIO

1. INTRODUÇÃO AOS NÚMEROS PRIMOS

1.1. IMPORTÂNCIA DOS NÚMEROS PRIMOS

Os números primos são a matéria prima na formação de todos os demais números. Sendo assim, são eles objetos de estudos ininterruptos desde os primórdios.

Entretanto, os números primos guardam segredos que por vezes nos parecem intransponíveis, sendo considerados por alguns como o assunto mais misterioso já estudado pelos matemáticos. No início do Século XX, David Hilbert, professor da Universidade de Göttingen e um dos maiores matemáticos da época, proferiu uma palestra no Congresso Internacional de Matemáticos, realizado em agosto de 1900, na Sorbone. Em sua palestra, Hilbert falou sobre o desconhecido, sobre os desafios da matemática no século que se iniciava. Ele desafiou a plateia de ilustres matemáticos com uma lista de 23 problemas, que segundo ele, ditariam o futuro das pesquisas matemáticas. Muitos desses problemas encontraram resposta ao longo das décadas seguintes, porém, o oitavo problema, até hoje não foi solucionado. Trata-se de provar a Hipótese de Riemann, assunto que trataremos mais adiante.

Embora complexos e misteriosos, os números primos têm um caráter atemporal e universal, eles não foram inventados pelo homem, nós apenas atribuímos nomenclaturas e buscamos continuamente aprofundar no conhecimento dos seus mistérios.

Por seu caráter atemporal e universal, os números primos são considerados o código que poderia ser compreendido por seres inteligentes extraterrenos. Por isso, a sequência dos primeiros números primos foi gravada em um disco de ouro e cobre enviado na primeira nave espacial a sair do sistema solar. O disco continha também diversas imagens do nosso planeta, imagens indicando a

nossa localização no sistema solar, além de sons, músicas e frases em diversos idiomas. Mas de tudo isso, a sequência de números primos foi considerado o código com maior possibilidade de ser reconhecido. No clássico romance *Contato* de Carl Sagan os alienígenas usam os números primos para fazer contato com a Terra. A heroína, Ellie Arroway, reconhece imediatamente o pulsar do sinal de rádio receptado.

Estes e outros números são estudados na disciplina Teoria dos Números, que é considerada uma das mais difíceis de toda a Matemática, por utilizar técnicas sofisticadas e Matemática avançada. Até os anos 1970, a Teoria dos Números foi considerada uma disciplina com pouca aplicação prática. Nesta década porém, os cientistas Ron Rivest, Adi Shamir e Leonard Adleman desenvolveram uma forma de utilizar os números primos na construção de métodos de codificação em Criptografia. Voltaremos a este assunto mais tarde.

1.2. DEFINIÇÃO DE NÚMEROS PRIMOS

Definição: Um número inteiro n ($n > 1$) é dito um número primo, se possuir exatamente dois divisores positivos, a saber, 1 e n.

O número 1, só possui um divisor, ele mesmo. Não sendo, portanto, um número primo.

Todos os demais números inteiros maiores que 1 e não primos, possuem mais de dois divisores. Eles são chamados de números compostos, logo, poderão ser fatorados em seus elementos constituintes. Estes elementos serão necessariamente números primos conforme enuncia o Teorema Fundamental da Aritmética.

Teorema (*Teorema Fundamental da Aritmética*): Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto

$$n = p_1 \dots p_m$$

O $m \geq 1$ é um natural e $p_1 \leq \cdots \leq p_m$ são primos.

Podemos então dizer que os números primos são os elementos de formação de todos os demais números, podendo ser considerados os próprios átomos da aritmética, ou ainda os tijolos na construção numérica, construção essa feita por meio da operação de multiplicação.

O Teorema Fundamental da Aritmética faz duas afirmações que demostraremos a seguir:

1ª Todo número $n > 1$ pode ser representado como um produto de primos

$n = \prod_{n=1}^{r} p_n, r \geq 1,$

ou seja, existe uma fatoração de n em números primos.

2ª Esta representação é única a não ser pela ordem dos fatores. Ou seja, todo primo que aparece em uma decomposição em "fatores primos" de um dado número aparece com frequência igual em qualquer decomposição dessas.

Todo $n > 1$ pode ser escrito:

$$n = \prod_{p|n} p^l,$$

onde p percorre os vários primos que dividem n; e onde $l = l_{a,p} > 0$, é unicamente determinado por n e por p. (Esta é a chamada Decomposição Canônica).

Demostramos a existência da fatoração de n em primos por indução matemática.

i) Se n é primo não há o que provar (escrevemos $m = 1,\ p_1 = n$).

ii) Se n é composto podemos escrever:

$n = ab,\ sendo: a, b \in \mathbb{N},\ 1 < a < n,\ 1 < b < n.$

Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n. □

Antes de demonstrar a unicidade da representação, precisamos introduzir um novo teorema.

Teorema: Se:

$$p \mid \prod_{i=1}^{v} n_i \,,$$

Então para ao menos um valor de i temos:

$$p|n_i \,.$$

Para demonstrarmos a unicidade da representação, basta provar que, se:

$$n = \prod_{i=1}^{v} p_i = \prod_{i=1}^{v'} p'_i \,,$$

$$p_1 \leq p_2 \leq \cdots \leq p_v \,, \qquad p'_1 \leq p'_2 \leq \cdots \leq p'_{v'}$$

Então:

$v = \boldsymbol{v'}, \quad \boldsymbol{p_i} = \boldsymbol{p'_i}$ para $1 \leq i \leq \boldsymbol{v}$.

Para $n = 2$ a afirmação é verdadeira, uma vez que temos:

$v = \boldsymbol{v'} = \mathbf{1}$ e $\boldsymbol{p_1} = \boldsymbol{p'_1} = \mathbf{2}$

Seja $n > 2$ e suponha que a afirmação foi provada para 2, 3, 4, ..., $n - 1$.

Se n for primo então:

$v = \boldsymbol{v'} = \mathbf{1}$, $\boldsymbol{p_1} = p_2 = n$

Caso contrário, temos $\boldsymbol{v} > 1$ e $\boldsymbol{v'} > 1$. Como

$$p'_1 | \prod_{i=1}^{v} p_i,$$

e

$$p_1 | \prod_{i=1}^{v'} p'_i$$

Segue do teorema apresentado que:

$p'_1 = p_i$ e $p_1 = p'_m$

Para pelo menos um i e pelo menos m. Como:

$$p_1 \leq p_i = p'_1 \leq p'_m = p_1$$

Temos:

$$p_1 = p'_1$$

Agora, como $1 < p_1 < n$, $p_1 \mid n$, temos:

$$1 < \frac{n}{p_1} = \prod_{i=2}^{v} p_i = \prod_{i=2}^{v'} p'_i < n,$$

e logo, pela hipótese de indução,

$$\boldsymbol{v - 1 = v' - 1}, \quad \boldsymbol{v = v}$$

e

$$p_i = p'_i \quad para\ 2 \leq i \leq \boldsymbol{v}$$

□

2. A INFINITUDE DOS NÚMEROS PRIMOS

Os números primos suscitam muitas questões. Uma delas é: “Quantos números primos existem? Eles formam um conjunto finito ou existe uma infinidade de números primos?”

Notícias sobre a última descoberta do maior número primo conhecido são recorrentes. Marcus du SAUTOY, em A Música dos Números Primos – A História de Um Problema não Resolvido na Matemática **(**DU SAUTOY, 2007), se refere a um recorte de jornal guardado com muito cuidado pela matemática Julia Robinson e intitulado ENCONTRADO O MAIOR NÚMERO, que nos mostra que, “mesmo na década de 1930, até as descobertas incorretas chegavam às notícias”.

Entretanto, diversas provas de que existe uma infinidade de números primos já foram formuladas. A mais ilustre é a demonstração de Euclides, que a mais de 2.300 anos demonstrou que

os números primos são infinitos, em uma demonstração considerada uma das mais belas e elegantes em toda a matemática. Esta demonstração consta dos Elementos de Euclides que foram escritos por volta de 300 a.C.

Apresentaremos a seguir três dessas demonstrações, outras tantas estão disponíveis na literatura sobre o tema, algumas de matemáticos famosos, outras de matemáticos que caíram no esquecimento.

2.1. DEMONSTRAÇÃO DE EUCLIDES

Os gregos evitavam lidar com o conceito de infinito, pelas dificuldades que esse conceito sempre causava, assim na Proposição 20 do Livro 9 dos *Elementos de Euclides* demonstrou que dado qualquer conjunto de primos, sempre existe um número primo fora deste conjunto, o que significa dizer que o conjunto de números primos é infinito (ÁVILA, 2010).

Suponhamos que o conjunto de primos seja finito. Sendo a sequência $P = p_1, p_2, \dots, p_r$ a lista de todos os primos.

Consideremos o número $N = p_1 \, . \, p_2 \, . \dots . \, p_r + 1$. Nenhum dos primos da sequência finita P pode dividi-lo exatamente, sempre sobrará um resto 1.

Dado que todos os números compostos podem ser construídos pela multiplicação de primos, o número formado N ou é um novo primo ou é gerado por um primo não pertencente ao conjunto finito denominado por P.

Portanto, a sequência de primos não pode ser finita.

2.2. DEMONSTRAÇÃO DE GOLDBACH

A demonstração de Goldbach se tornou conhecida após sua publicação em Berlim em 1924, entretanto ela se encontra em uma carta de C. Goldbach a Euler datada de 21/31 julho 1730. Em 1891, A. Hurwitz descobriu independentemente a mesma demonstração em um exercício (RIBENBOIM, 2012).

Ela utiliza a seguinte ideia: basta achar uma sucessão infinita $a_1 < a_2 < a_3 < \cdots$ de números naturais, primos entre si, dois a dois, isto é sem fator primo comum. Se p_1 é um fator primo de a_1, p_2 um fator primo de a_2, ... , p_n um fator primo de a_n , então $p_1, p_2, \ldots, p_n$, ... são todos distintos.

Os números de Fermat $F_n = 2^{2^n} + 1$ (para $n \geq 0$) são uma sucessão infinita e primos entre si, dois a dois.

Demonstração: Por recorrência sobre m, é fácil ver que, $F_m - 2 = F_0 F_1 \ldots F_{m-1}$; então se $n < m$, F_n divide $F_m - 2$. Se um número primo p dividisse simultaneamente F_n e F_m, dividiria igualmente $F_m - 2$ e portanto 2 e então $p = 2$, o que é impossível porque F_m é impar. Os números e o Teorema de Fermat serão tratados mais adiante.

□

2.3. DEMONSTRAÇÃO DE EULER

Euler mostrou que existe uma infinidade de números primos, estabelecendo que uma determinada expressão formada com números primos era infinita. Se p é um número primo qualquer, então $1/p < 1$. Então a soma da série geométrica de razão $1/p$ e primeiro termo 1 é dada por:

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1-p^{-1}}.$$

Igualmente, se q é outro número primo, então:

$$\sum_{k=0}^{\infty} \frac{1}{q^k} = \frac{1}{1-p^{-1}}.$$

Multiplicando membro a membro, essas duas igualdades, obtemos:

$$1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{p^2} + \frac{1}{pq} + \frac{1}{q^2} + \cdots = \frac{1}{1-p^{-1}} \times \frac{1}{1-p^{-1}}.$$

O primeiro membro é a soma dos inversos de todos os inteiros naturais da forma $p^h q^k$ (com $h \geq 0, k \geq 0$), cada um sendo contado uma única vez, porque a expressão de cada número natural, como produtos de primos é única.

A demonstração de Euler diz o seguinte:

Supõe-se que $p_1, p_2, \ldots, p_r$ formam a totalidade dos números primos. Para cada $i = 1, 2, \cdots, r$, tem-se:

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1-p_i^{-1}}.$$

Multiplicando, membro a membro, essas r igualdades, obtém-se:

$$\prod_{i=1}^{r} \left(\sum_{k=0}^{\infty} \frac{1}{p_i^k} \right) = \prod_{i=1}^{r} \frac{1}{1-p_i^{-1}}.$$

E o primeiro membro, uma vez efetuadas as operações, é a soma dos inversos de todos os números naturais, cada um contado uma única vez, como resulta do teorema fundamental que estabelece que cada número composto se escreve de maneira única (a menos de permutações) como produto de fatores primos.

É sabido que a série $\sum_{n=1}^{\infty}(\,{}^{1}/_{n}\,)$ é divergente e, como seus termos são positivos, a ordem da soma desses termos é irrelevante; o primeiro membro da igualdade será então infinito, enquanto seu segundo membro será finito. Isso é absurdo!

□

3. COMO RECONHECER UM NÚMERO PRIMO

As questões sobre como reconhecer um número primo e, em sendo um número composto, como decompô-lo em seus fatores primos foram formuladas em tempos remotos. Karl Friedrich Gauss escreveu no artigo 329 das *Disquisitiones Arithmeticae* (1801): "O problema de distinguir números primos de compostos e de decompor esses últimos em seus fatores primos é conhecido como sendo um dos mais importantes e úteis na aritmética... A dignidade da própria ciência parece requerer que todos os meios possíveis sejam explorados para a solução de um problema tão elegante e tão celebrado" (MARTINEZ; MOREIRA; SALDANHA; TENGAN, 2011).

3.1. O CRIVO DE ERATÓSTENES

A maneira aparentemente mais simples e intuitiva de verificar se um determinado número natural é primo é conhecida como o Crivo de Eratóstenes. Erastóstenes, diretor da biblioteca do grande instituto de pesquisa da Grécia Antiga em Alexandria, no século III a.C., foi a primeira pessoa a produzir tabelas de números primos (DU SAUTOY, 2007). A técnica por ele utilizada foi bastante

simples e intuitiva. Ele escrevia inicialmente os números de 1 a N. Em seguida, escolhia o primeiro primo (2) e eliminava da lista todos os seus múltiplos. Passava, então ao próximo número não eliminado, 3, e eliminava também todos os seus múltiplos. Repetia sucessivamente este método até o maior inteiro inferior a $\sqrt{N}$ e cada novo primo que encontrava gerava um crivo que era utilizado para eliminar os números compostos múltiplos desse crivo (RIBENBOIM, 2011).

Os números não primos da relação eram então decompostos da seguinte forma. Seja N um número composto identificado divisível por N_0, ele pode ser escrito como $N = N_0 * N_1$, onde $N_1 < N$, e repete-se o mesmo processo para N_0 e para N_1. Esse algoritmo fornece a decomposição de N em fatores primos.

Esse método pode ser utilizado para gerar tabelas de primos relativamente grandes, porém para valores muito grandes de N, o algoritmo exige muito tempo e cálculos para verificar se é um número primo ou composto. Surge então a necessidade de encontrar um algoritmo eficaz, ou seja, que exija menos tempo e menor custo, para execução.

3.2. TEOREMAS FUNDAMENTAIS SOBRE CONGRUÊNCIAS

Os métodos para testar a primariedade de um número e para determinar seus fatores primos, caso não seja primo, se apoiam em teoremas sobre congruências, em particular sobre o Pequeno Teorema de Fermat, Teorema de Wilson e o Teorema de Euler (generalização do Pequeno Teorema de Fermat).

Pequeno teorema de Fermat: Se p é um número primo e se a é um número natural, então $a^p \equiv a\ (mod\ p)$. Em particular, se p não divide a, então $a^{p-1} \equiv 1\ (mod\ p)$.

A demonstração deste teorema pode ser encontrada em *Teoria dos Números* (SANTOS, 2011).

Teorema de Wilson: Seja $p > 1$, então $p \mid (p-1)! + 1$ se, e somente se, p for primo. O que é o mesmo que dizer: se p é primo, então $(p-1)! \equiv -1\ (mod\ p)$.

Demonstração:

Para $p = 2$ é óbvio: $1 \equiv -1(2)$

Pelo Teorema de Fermat:

Para $p \neq 2$

$$x^{p-1} - \overline{1} = (x - \overline{1})(x - \overline{2}) - \cdots - \left(x - (\overline{p-1})\right)$$

Comparando os coeficientes constantes temos:

$$-\overline{1} = (-1)^{p-1}\ \overline{(p-1)}\ !$$

O Teorema de Wilson fornece uma caracterização dos números primos, entretanto, a identificação dos primos com base neste teorema não é prática, pois não se conhece um algoritmo para calcular rapidamente o fatorial de um número. O único algoritmo conhecido é o da definição de fatorial que gera cálculos extensos, quando se trabalha com números muito grandes.

O Teorema de Euler é uma generalização do Pequeno Teorema de Fermat, através da introdução da função tociente (φ) ou função de Euler.

A função φ de Euler pode ser definida por: seja n é um inteiro positivo, $\varphi(n)$ será o número de inteiros positivos menores ou iguais a n que são relativamente primos com n.

O **Teorema de Euler** diz que: Se m é um inteiro positivo e a um inteiro com $mdc\ (a, m) = 1$, ou seja, a e m são primos entre si, então

$$a^{\varphi(m)} \equiv 1\ (mod\ m)$$

A demonstração do teorema de Euler também pode ser encontrada na obra citada anteriormente (SANTOS, 2011).

Como para p primo, $\varphi(p) = p - 1$, o Teorema de Euler é uma generalização do Pequeno Teorema de Fermat, como dito anteriormente.

Como mencionado na introdução, os números primos são utilizados no método de Criptografia RSA. Esse método é um caso prático de aplicação do Teorema de Euler.

Segue uma descrição resumida do método:

- Receptor publica um inteiro N , onde $N = pq$, sendo p e q primos grandes.
- N é público, mas sua fatoração pq só é conhecida pelo receptor.
- Receptor publica um expoente s (não muito grande) sendo:

$mdc\left(s, (p-1)(q-1)\right) = 1$

- Receptor (usando o algoritmo de Euclides) calcula:

Inverso de $s\ mod\ (p-1)(q-1) = \varphi(N)$

Isto é, um número natural r < (p-1)(q-1) com $rs \equiv 1(mod\ (p-1)(q-1))$

(Donde $rs = 1 + k\varphi(N)$, para algum natural k)

Note que apesar de N e s serem públicos, não parece ser fácil calcular $\varphi(N)$ ou r (neste contexto, calcular $\varphi(N) = (p-1)(q-1)$ dado $N = pq$ é equivalente a fatorar N, isto é, a encontrar os fatores primos p e q).

- Uma mensagem é um número natural $n < N$.
- O emissor envia $\tilde{n} := m^s (mod\ N)$, com $0 < \tilde{n} < N$.
- O receptor recupera n via: $n \equiv \tilde{n}^r\ (mod\ N)$

Para verificar essa equivalência, podemos observar que:

$$\tilde{n}^r \equiv (n^s)^r = n^{rs} = n^{1+k(p-1)(q-1)} = m \cdot (n^{p-1})^{k(q-1)} \equiv n\ (mod\ p)$$

Note que, se $p|n$, os dois lados são $0\ mod\ p$, e, caso contrário, $n^{p-1} \equiv 1\ (mod\ p)$; analogamente $\tilde{n}^r \equiv m\ (mod\ q)$, donde $\tilde{n}^r \equiv n\ (mod\ N)$.

Mais detalhes sobre Criptografia RSA podem ser encontrados em Teoria dos Números – Um passeio com primos e outros números familiares pelo mundo inteiro (MARTINEZ; MOREIRA; SALDANHA; TENGAN, 2011).

3.3. TESTES DE PRIMALIDADE

Uma questão de muita importância em Teoria dos Números é identificar se um determinado número é primo ou composto. Para números pequenos é bastante simples, bastando aplicar o algoritmo do Crivo de Eratóstenes. Entretanto, para números grandes, este método é muito lento e se torna praticamente inviável com a tecnologia de computação hoje disponível.

O Teorema de Wilson, como dito anteriormente, seria uma boa opção, porém calcular o fatorial de números grandes é igualmente trabalhoso.

Outra ideia é utilizar o Pequeno Teorema de Fermat que nos diz que, se p é primo e a um número natural, não múltiplo de p, então $a^{p-1} \equiv 1\ (mod\ p)$. Entretanto, a recíproca não é verdadeira. Existem números compostos N e $a \geq 2$, tais que $a^{N-1} \equiv 1(mod\ N)$. Estes números são chamados pseudoprimos na base a.

Pseudoprimos existem, mas são raros. Por exemplo o menor pseudoprimo na base 2 é $341 = 11\ x\ 31$ e existem apenas 21.853 pseudoprimos na base 2 menores que $2{,}5\ x\ 10^{10}$, contra 1.091.987,405 primos (MARTINEZ et. Al., 2011).

Uma recíproca do Pequeno Teorema de Fermat foi descoberta por Lucas em 1876, e será o primeiro teste apresentado (RIBENBOIM, 2012).

Teste 1: Seja $N > 1$. Supõe-se que exista um inteiro $a > 1$ tal que:

(i) $a^{N-1} \equiv 1\ mod\ (N)$,

(ii) $a^m \not\equiv 1\ (mod\ N)\ \ para\ m = 1, 2, \cdots, N-2$

Então N é primo!

Defeito do Teste: Também exige muitas operações. $N - 2$ multiplicações sucessivas por a e a verificação que 1 não é resíduo módulo N de uma potência de a inferior a $N - 1$.

Demonstração: Basta mostrar que todo inteiro $m,\ 1 \leq m < N$ é primo com N, isto é, $\varphi(N) = N - 1$. Com esse objetivo, basta mostrar que existe $a, 1 \leq a < N, mdc\ (a, N) = 1$, tal que a ordem de a módulo N seja $N - 1$. Isto é exatamente o que exprime a hipótese.

□

Em 1891, Lucas formulou um outro teste (RIBENBOIM, 2012):

Teste 2: Seja $N > 1$. Supõe-se que exista um inteiro $a > 1$, tal que:

(i) $a^{N-1} \equiv 1\ (mod\ N)$,

(ii) $a^m \not\equiv 1 (mod\ N)\ para\ \ todo\ \ divisor\ m\ de\ N - 1.$

Então N é primo!

Defeito do Teste: O teste exige o conhecimento de todos os fatores de $N - 1$; não se pode aplicá-lo facilmente, exceto quando N tem uma forma particular, como por exemplo $N = 2^n + 1$ ou $N = 3\ x\ 2^n + 1$.

Demonstração: Mesma do teste 1.

Em 1967, Brillhart e Selfridge tornaram o teste de Lucas mais flexível (RIBENBOIM, 2012):

Teste 3: Seja $N > 1$. Supõe-se que, para todo fator primo q de $N - 1$, exista um inteiro $a = a(q) > 1$, tal que:

(i) $a^{N-1} \equiv 1\ (mod\ N)$,

(ii) $a^{(N-1)/q} \not\equiv 1\ (mod\ N)$.

Então, N é primo.

Defeito do Teste: Ainda é necessário conhecer os fatores primos de $N-1$, mas o número de congruências para examinar é menor.

Demonstração: Basta demonstrar que $\varphi(N) = N-1$, e , como $\varphi(N) \leq N-1$, é suficiente mostrar que $N-1$ divide $\varphi(N)$. Se fosse falso, existiria um número primo q e um inteiro $r \geq 1$ tais que q^r divide $N-1$, enquanto q^r não dividiria $\varphi(N)$.

Seja $a = a(q)$ e seja e a ordem de a módulo N. Então e divide $N-1$ e e não divide $(N-1)/q$, e, consequentemente, q^r divide e. Como $a^{\varphi(N)} \equiv 1\ mod\ (N)$, então e divide $\varphi(N)$, então $q^r \mid \varphi(N)$, o que é uma contradição e assim termina a demonstração!

□

Os três testes apresentados até agora apresentam como limitação a necessidade de se determinar os fatores primos de $N-1$, operação que pode não ser tão fácil de se realizar. Apresentaremos então mais dois testes que requerem apenas a fatoração parcial de $N-1$. Esses testes se baseiam nas seguintes proposições feitas por Pocklington em 1914 sobre fatores primos.

1ª Proposição – Seja $N-1 = q^n R$, onde q é primo, $n \geq 1$ e q não divide R. Supõe-se a existência de inteiro $a > 1$, tal que:

(i) $a^{N-1} \equiv 1\ (mod\ N)$,

(ii) $mdc\left(a^{(N-1)/q} - 1, N\right) = 1$.

Então, todo fator primo de N é da forma $mq^n + 1$, com $m \geq 1$.

Demonstração: Seja p um fator primo de N e seja e a ordem de a módulo p (ou seja, e é o menor inteiro positivo, tal que: $a^e \equiv 1\ mod\ p$), logo e divide $p-1$; pela condição *(ii)*, e não pode dividir $(N-1)/q$, porque p divide N; então q não divide $(N-1)/e$ e daí que q^n divide e e, a fortiori, q^n divide $p-1$.

□

Se se puder verificar que todo fator primo $p = mq^n + 1$, é maior que $\sqrt{N}$ então N é primo, Se q^n é bem grande, essa verificação pode ser feita em pouco tempo.

A segunda proposição de Pocklington, é uma melhoria do resultado (RIBENBOIM, 2012):

2ª Proposição: Seja $N-1=FR$ onde $mdc\,(F,R)=1$ e onde a fatoração de F é conhecida. Supõe-se que, para todo fator primo q de F, exista um inteiro $a=a(q)>1$, tal que:

(i) $a^{N-1}\equiv 1\,(mod\,N)$,

(ii) $mdc\left(a^{(N-1)/q}-1,N\right)=1$.

Então, todo fator primo de N é da forma $mF+1$, com $m\geq 1$.

Os mesmos comentários de aplicam a essa situação. Em particular, se $F>\sqrt{N}$, então N é primo.

Os dois testes a seguir são consequências dessas proposições e foram propostos por Proth em 1878. Como dito anteriormente estes testes necessitam do conhecimento dos fatores primos de $N-1$ (RIBENBOIM, 2012).

Teste 4: Seja $N=2^nh+1$, com h ímpar e $2^n>h$. Supõe-se que exista um inteiro $a>1$ tal que $a^{(N-1)/2}\equiv -1\,(mod\,N)$. Então N é primo.

Demonstração: $N-1=2^nh$ com h ímpar e $a^{N-1}\equiv 1\,(mod\,N)$. Sendo dado que N é ímpar, então $mdc\left(a^{(N-1)/2}-1,N\right)=1$. Pelo resultado acima, cada fator primo p de N é da forma $p=2^nm+1>2^n$. Ora, $N-2^nh+1<2^{2n}$, daí $\sqrt{N}<2^n<p$ e, por consequência, N é primo!

□

Teste 5: Seja $N-1=FR$ com $mdc\,(F,R)=1$, a fatoração de F suposta conhecida: B é um inteiro tal que $FB>\sqrt{N}$ e R sem qualquer fator primo inferior a B. Também se supões:

(i) para cada fator primo q de F, existe um inteiro $a=a(q)>1$, tal que $a^{N-1}\equiv 1\,(mod\,N)$ e $mdc\left(a^{(N-1)/q}-1,N\right)=1$.

(ii) existe um inteiro $b>1$ tal que $b^{N-1}\equiv 1\,(mod\,N)$ e $mdc\,(b^F-1,N)=1$.

Então, N é primo.

Demonstração: Seja p um fator primo de N, seja e a ordem de b módulo N; então e divide $p-1$ e e também divide $N-1=FR$. Sendo dado que e não divide F, então $mdc\ (e,R) \neq 1$ e daí, existe um número primo q tal que $q \mid e$ e $q \mid R$ e, então, q divide $p-1$. Entretanto, pelo resultado precedente, F divide $p-1$; sendo dado que $mdc\ (F,R)=1$, qF divide $p-1$. Assim, $p-1 \geq qF \geq BF > \sqrt{N}$. Isto acarreta que $p=N$ e então N é primo!

□

ALGORITMO AKS

No final de 2002, um professor indiano, Manindra Agrawal, e seus dois alunos, Neeraj Kayal e Nitin Saxena, descobriram um algoritmo que está sendo chamado de AKS (iniciais de seus nomes), que permite verificar, sem margem de erro, se um inteiro positivo é ou não primo, em tempo polinomial.

O algoritmo AKS ganhou destaque por ser o primeiro algoritmo publicado que é simultaneamente polinomial, determinístico, e incondicional. O que isto significa, o tempo máximo de processamento do algoritmo pode ser expresso como um polinômio em relação ao número de dígitos do número analisado. Isto permite classificar o número informado como primo ou composto ao invés de retornar um resultado probabilístico. (FARIAS, PUC BRASILIA)

4. DISTRIBUIÇÃO DOS NÚMEROS PRIMOS

Uma das questões sobre os números primos que desaviam os matemáticos diz respeito à distribuição dos números primos. Existe alguma lógica que nos permita prever como os números primos se distribuem? É possível determinar o enésimo número primo? Podemos dizer quantos números primos existem inferiores a um dado número N?

À primeira vista a distribuição dos primos nos parece totalmente aleatória. A Tabela 1 apresenta a relação de números primos até 1009. Visualmente não é possível perceber qualquer regularidade. Quando analisamos os 100 primeiros números antes de 10.000.000, encontramos 9 números primos, porém dentre os 100 primeiros números depois de 10.000.000, encontramos apenas 2.

Tabela 1: Números Primos até 1.009

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	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	

Mas, para os matemáticos, alguns exemplos não bastam, eles seguem buscando padrões e estruturas no mundo dos números. No caso particular dos números primos essa busca se iniciou ha muito tempo atrás e ainda persiste como um mistério que a natureza ainda não se dispôs a revelar, embora progressos tenham sido feitos. A seguir faremos um relato histórico das descobertas sobre o tema, conforme Ribenboim em Números Primos – Velhos Mistérios, Novos Recordes (RIBENBOIM, 2012).

Chamaremos de $\pi(x)$ a função de contagem dos números primos, ou seja, para todo número $x > 0$, deseigna-se por $\pi(x)$ o número de primos p tais que $p \leq x$.

Com base nesta definição, o que se espera é que uma dada função que nos retorne $\pi(x)$, os valores obtidos sejam tão próximos quanto possível de $\pi(x)$. Isso não é fácil, até o presente momento todas as funções fornecem aproximações de $\pi(x)$, desta forma, sempre existirá algum erro. Então para cada função deve-se estimar o erro.

4.1. EULER

Começamos nosso relato histórico com Euler. Euler observou que, para todo número real $\sigma > 1$, a série (RIBENBOIM, 2012):

$$\sum_{n=1}^{\infty} \frac{1}{n^{\sigma}}$$

É convergente.

Observou também que para todo $\sigma_0 > 1$, ela é uniformemente convergente na semirreta $\sigma_0 \leq \sigma < \infty$. Assim, essa série define uma função $\zeta(\sigma)$, chamada *função zeta*, para $1 < \sigma < \infty$, que é contínua e diferenciável. Além disso,

$$\lim_{\sigma \to \infty} \zeta(\sigma) = 1 \quad \text{e} \quad \lim_{\sigma \to 1+0} (\sigma - 1)\zeta(\sigma) = 1.$$

A ligação entre a função zeta e os números primos é uma expressão analítica da fatoração única de inteiros como produto de números primos:

$$\zeta(\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}} = \prod_{p} \frac{1}{1 - \frac{1}{p^{\sigma}}}, \text{para } \sigma > 1$$

$$\prod_p \frac{1}{1-\frac{1}{p^\sigma}} = \prod (1 + p^{-\sigma} + p^{-2\sigma} + \cdots)$$

Expandindo o último produto, temos:

$$\zeta(\sigma) = \sum_{v=1}^{+\infty} v^{-\sigma}$$

Uma vez que cada número inteiro $v \geq 1$ pode ser exclusivamente expresso como um produto de potência de primos racionais. Além disso, temos, para $\sigma > 1$:

$$1 < \zeta(\sigma) < 1 + \sum_{v=2}^{+\infty} \int_{v-1}^{v} t^{-\sigma} dt = 1 + \int_1^{+\infty} t^{-\sigma} dt = 1 + (\sigma - 1)^{-1}$$

O que mostra que $\zeta(\sigma)$ é convergente para $\sigma > 1$ e tende para 1 quando $\sigma \to +\infty$ (WEIL, 1974).

Daí se conclui que $\zeta(\sigma) \neq 0$ para $\sigma > 1$.

Euler demonstrou também que a soma dos inversos dos números primos é divergente:

$$\sum_p \frac{1}{p} = \infty$$

Demonstração: Seja N um número natural arbitrário. Todo inteiro $n \leq N$ é o produto, que se obtém de modo único, de potências de números primos $p \leq n$. Igualmente, para cada primo p.

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1-\frac{1}{p}}.$$

Então:

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{p \leq N} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right) = \prod_{p \leq N} \frac{1}{1-\frac{1}{p}}.$$

Mas:

$$\log \prod_{p \le N} \frac{1}{1-\frac{1}{p}} = -\sum_{p \le N} \log\left(1-\frac{1}{p}\right).$$

E, para cada primo p:

$$-\log\left(1-\frac{1}{p}\right) = \sum_{m=1}^{\infty} \frac{1}{mp^m} \le \frac{1}{p} + \frac{1}{p^2}\left(\sum_{h=0}^{\infty} \frac{1}{p^h}\right) =$$

$$= \frac{1}{p} + \frac{1}{p^2} x \frac{1}{1-\frac{1}{p}} = \frac{1}{p} + \frac{1}{p(p-1)}$$

$$< \frac{1}{p} + \frac{1}{(p-1)^2}.$$

Então:

$$\log \sum_{n=1}^{N} \frac{1}{n} \le \log \prod_{p \le N} \frac{1}{1-\frac{1}{p}} \le \sum_{p \le N} \frac{1}{p} + \sum_{p \le N} \frac{1}{(p-1)^2} \le \sum_{p} \frac{1}{p} + \sum_{n=1}^{\infty} \frac{1}{n^2}.$$

□

∑ 1/p diverge onde a soma é sobre todos os primos positivos em $\mathbb{Z}$.

Seja $p_1, p_2, \dots, p_{l(n)}$ todos os números primos menores que n definido por $\lambda(n) = \prod_{i=1}^{l(n)} (1-\frac{1}{p_i})^{-1}$. Se $(1-\frac{1}{p_i})^{-1} = \prod_{a_i}^{\infty} = 0^{1/p_i{}^{a_i}}$ vemos que $\lambda(n) = \sum (p_1^{a1} p_2^{a2} \dots \dots p_l^{a1})^{-1}$,

Onde a somatória é válida para todo l de integrais não negativas ($a_1, a_2, \dots, a_l$).

Em particular se percebe que $1 + \frac{1}{2} + \frac{1}{3} + \cdots + 1/n < \lambda(n)$. Assim $\lambda(n) \to \infty$ como $n \to \infty$.

Isto já comprova que existe infinitos primos.

Considerando $log\ \lambda(n)$ temos

$log\ \lambda(\mathrm{n}) = -\sum_{\mathrm{i}=1}^{\mathrm{l}} \log\ (1-\mathrm{p_i^{-1}}) = \sum_{\mathrm{i}=1}^{\mathrm{l}} \sum_{\mathrm{m}=1}^{\infty} (\mathrm{mp_i^m})^{-1} = \mathrm{p_1^{-1}} + \mathrm{p_2^{-1}} + \cdots + \mathrm{p_l^{-1}} + \sum_{\mathrm{i}=1}^{\mathrm{l}} \sum_{\mathrm{m}=2}^{\infty} (\mathrm{mp_i^m})^{-1}$

Agora, $\sum_{\mathrm{m}=2}^{\infty} (\mathrm{mp_i^m})^{-1} < \sum_{\mathrm{m}=2}^{\infty} \mathrm{p_i^{-m}} = \mathrm{p_i^{-2}}\,(1-\mathrm{p_i^{-1}})^{-1} \leq 2\mathrm{p_i^{-2}}$.

Assim $log\ (\lambda) < \mathrm{p_1^{-1}}\ \mathrm{p_2^{-1}} + \cdots + \mathrm{p_l^{-1}} + 2\,(\mathrm{p_1^{-2}} + \mathrm{p_2^{-2}} + \cdots + \mathrm{p_l^{-2}})$.

É sabido que $\sum_{\mathrm{n}=1}^{\infty} \mathrm{n^{-2}}$ converge.

Segue-se que $\sum_{\mathrm{i}=1}^{\infty} \mathrm{p_i^{-2}}$ converge.

Assim se $\sum \mathrm{p^{-1}}$ converge, haveria uma constante M de modo que $\log \lambda(\mathrm{n}) < M$, ou $\lambda(\mathrm{n}) < \mathrm{e^M}$.

Isso é impossível pois $\lambda(\mathrm{n}) \to \infty$ e $\mathrm{n} \to \infty$.

Logo $\sum \mathrm{p^{-1}}$ diverge.

□

Mas a série $\sum_{n=1}^{\infty}(1/n^2)$ é convergente. Como N é arbitrário e a série harmônica $\sum_{n=1}^{\infty}(1/n)$ é divergente, $\log \sum_{n=1}^{\infty}(1/n = \infty)$ e, em consequência, a série $\sum_p(1/p)$ é divergente.

Como a série $\sum_{n=1}^{\infty}(1/n^2)$ é convergente, pode-se então dizer que os quadrados são “mais frequentes” que os números primos.

Uma das belas descobertas de Euler é a soma da série:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Euler também calculou as somas de $\sum_{n=1}^{\infty}(1/n^{2k})$ para todo $k \geq 1$, dando assim a solução de um problema que desafiava os matemáticos da época, e obteve:

$$\zeta(2k) = \sum_{n\geq 1}^{\infty} \frac{1}{n^{2k}} = \frac{2^{2k-1}}{(2k)!} B_k \pi^{2k}$$

Para fazê-lo utilizou os números de Bernoulli, que são definidos da seguinte forma:

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad \cdots$$

E B_k é definido pela relação:

$$\binom{k+1}{1} B_k + \binom{k+1}{2} B_{k-1} + \cdots + \binom{k+1}{k} B_1 + B_0 = 0.$$

Esses números são racionais e é fácil ver que $B_{2k+1} = 0$ para todo $k \geq 1$. Eles aparecem também como coeficientes do seguinte desenvolvimento de Taylor:

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} x^k = 1 - \frac{x}{2} + \sum_{k \geq 1} (-1)^{k+1} B_k \frac{x^{2k}}{(2k)!}$$

Por meio da fórmula de Stirling

$$n! \sim \frac{\sqrt{2\pi} n^{n+\frac{1}{2}}}{e^n}, \quad \text{quando} \quad n \to \infty.$$

pode-se mostrar que:

$$|B_{2n}| \sim 4\sqrt{\pi n} \left(\frac{n}{\pi e}\right)^{2n}.$$

A série acima é então convergente no intervalo $|x| < 2\pi$.

Euler já havia utilizado os números de Bernoulli para representar somas de potências dadas de inteiros consecutivos:

$$\sum_{j=1}^{n} j^k = S_k(n), \qquad \text{para } k \geq 1.$$

Onde:

$$S_k(X) = \frac{1}{k+1} \left[X^{k+1} - \binom{k+1}{1} B_1 X^k + \binom{k+1}{2} B_2 X^{k-1} + \cdots + \binom{k+1}{k} B_k X \right].$$

A fórmula de Euler dando o valor de $\zeta(2K)$ é:

$$\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = (-1)^{k+1} \frac{(2\pi)^{2k} B_{2k}}{2(2k)!}.$$

Em particular:

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi}{6},$$

$$\zeta(4) = \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90},$$

etc.

Euler também considerou os polinômios de Bernoulli, que são assim definidos:

$$B_k(X) = \sum_{i=0}^{k} \binom{k}{i} B_i X^{k-i}, \qquad \text{para } k \geq 0.$$

Os polinômios $S_k(X)$ podem exprimir-se por meio dos polinômios de Bernoulli. Uma de suas mais importantes aplicações é uma generalização da fórmula do somatório de Abel, dando origem às fórmulas do somatório de Euler-MacLaurin, que lembramos aqui:

Se $f(x)$ é função contínua, tendo derivadas contínuas de ordem tão grande quanto necessário, se $a < b$ são inteiros, então, para todo $k > 1$,

$$\sum_{n=a+1}^{b} f(n) = \int_a^b f(t)dt + \sum_{r=1}^{k} (-1)^r \frac{B_r}{r!}\left(f^{(r-1)}(b) - f^{(r-1)}(a)\right)$$

$$+ \frac{(-1)^{k+1}}{k!} \int_a^b B_k(t - [t]) f^t(t)dt.$$

onde $[t]$ designa a parte inteira de t.

4.2. LEGENDRE

A primeira tentativa séria de estudo da função $\pi(x)$ (função de contagem dos números primos, como mencionado na introdução do item 4) é devida a Legendre (1808) que utilizou o crivo de Eratóstenes para mostrar que (RIBENBOIM, 2012):

$$\pi(N) = \pi\left(\sqrt{N}\right) - 1 + \sum \mu(d)\left[\frac{N}{d}\right].$$

O somatório refere-se a todos os divisores d do produto de todos os primos $p \leq \sqrt{N}$ e $\mu(x)$ é a função de Möbius, que é assim definida:

$$\mu_{(n)} = \begin{cases} 1, \quad Se \quad n = 1 \\ (-1)^r \ se\ n \text{ é } produto\ de\ r\ números\ primos\ distintos. \\ 0\ se\ n\ não \text{ é } livre\ de\ quadrados. \end{cases}$$

Como corolário, Legendre conjecturou em 1798 e em 1808, que:

$$\pi(x) \sim \frac{x}{\log x - A(x)},$$

Onde: $\lim_{x\to\infty} A(x) = 1{,}08366\cdots$

Tschebycheff mostrou, quarenta anos depois, que a conjectura de Legendre era falsa.

4.3. GAUSS

Na idade de 15 anos, em 1792, Gauss conjecturou que $\pi(x)$ era assintoticamente igual à função integral logarítmica, definida como (RIBENBOIM, 2012):

$$Li(x) = \int_2^x \frac{dt}{\log x}.$$

Sendo $Li(x) \sim x/\log x$, pode-se escrever a conjectura como:

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

Com o tempo, essa conjectura revelou-se verdadeira e esse fato é hoje conhecido como o Teorema dos Números Primos.

A aproximação de $\pi(x)$ por $x/\log x$ não é das melhores; a aproximação pela integral logarítmica é bem melhor.

4.4. TSCHEBYCHEFF

Um importante progresso para a determinação da ordem de grandeza da função $\pi(x)$ é devido a Tschebycheff, em 1850 (RIBENBOIM, 2012). Demonstrou ele, usando métodos elementares, que existem constantes C e C', $0 < C' < 1 < C$, tais que:

$$C' \frac{x}{\log x} < \pi(x) < C \frac{x}{logx} \qquad \text{para } x \geq 2.$$

Ele até calculou valores para C e C', todos muito próximos de 1. Assim, por exemplo, se $x \geq 30$, então as desigualdades acima valem com:

$$C' = \log \frac{2^{1/2} 3^{1/3} 5^{1/5}}{30^{1/30}} = 0{,}92129 \cdots,$$

$$C = \frac{6}{5} C' = 1{,}10555 \cdots$$

Por outro lado, se existir o

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

então ele deve ser igual a 1. Ele também concluiu que a aproximação de Legendre para $\pi(x)$ não podia estar correta.

Tschebycheff também demonstrou o postulado de Bertrand (1845), que afirma que, para todo número natural $n \geq 2$, existe um número primo entre n e seu dobro $2n$.

Ele estudou a função $\theta(x) = \sum_{p \leq x} \log p$, hoje chamada a Função de Tschebycheff, que dá essencialmente a mesma informação que $\pi(x)$, sendo, entretanto mais fácil de manipular.

A despeito do fato de Tschebycheff ter-se aproximado da demonstração do Teorema dos Fundamental dos Números Primos, conjecturado por Gauss, a demonstração se fez ainda esperar por cinquenta anos, até o fim do século. Neste entretempo, Riemann trouxe ideias novas e fundamentais à Teoria dos Números Primos.

4.5. RIEMANN

Riemann teve a ideia de definir a função zeta para todos os números complexos s, tendo parte real superior a 1, por (RIBENBOIM, 2012):

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{para } Re(s) > 1.$$

A fórmula do produto de Euler é ainda válida, para todo s tal que $Re(s) > 1$.

Por meio da fórmula do somatório de Euler e de MacLaurin, pode-se exprimir $\zeta(s)$ da seguinte maneira:

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + \sum_{r=2}^{k} \frac{B_r}{r!} s(s+1)\cdots(s+r-2) - \frac{1}{k!} s(s+1)\cdots(s+k-1) \int_1^{\infty} B_k(x - \{x\}) \frac{dx}{x^{s+k}}$$

Aqui, k é um número inteiro qualquer, $k \geq 1$, os números B_r são os de Bernoulli (não confundir com $B_k(x - [x])$, que é o valor do $k^{ésimo}$ polinômio de Bernoulli $B_k(X)$ em $x - [x]$).

A integral converge quando $Re(s) > 1 - k$; como k é um número natural qualquer, a fórmula fornece a extensão de $\zeta(s)$ no plano inteiro. $\zeta(s)$ é sempre holomorfa, exceto em $s = 1$, onde a função tem pólo simples, de resíduo igual a 1, isto é:

$$\lim_{s\to 1}(s-1)\zeta(s)=1.$$

Em 1859, Riemann encontrou a equação funcional para a função $\zeta(s)$. Como nessa equação intervém a função $\Gamma(s)$, vamos defini-la em primeiro lugar. Para $Re(s)>0$, uma definição conveniente utiliza a integral euleriana:

$$\Gamma(s)=\int_0^{\infty} e^{-u}u^{s-1}du.$$

Para números complexos arbitrários s, a função $\Gamma(s)$ pode ser definida do modo seguinte:

$$\Gamma(s)=\frac{1}{se^{\gamma s}}\prod_{n=1}^{\infty}\frac{e^{s/n}}{1+\frac{s}{n}}.$$

Onde γ é a constante de Euler, que é igual a:

$$\gamma=\lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right)=0{,}577215665\cdots$$

A constante de Euler está ligada ao produto de Euler pela seguinte fórmula devida a Mertens:

$$e^{\gamma}=\lim_{n\to\infty}\frac{1}{\log n}\prod_{i=1}^{\infty}\frac{1}{1-\frac{1}{p_i}}$$

$\Gamma(s)$ nunca vale 0; ela é sempre holomorfa, exceto nos pontos $0,-1,-2,-3,\cdots$ onde a função tem polos simples. Para todo inteiro positivo n, $\Gamma(x)=(n-1)!$; então a função gama é uma extensão da função fatorial.

A função gama satisfaz muitas relações interessantes, entre elas as equações funcionais:

$$\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin(\pi s)},\qquad \Gamma(s+1)=s\Gamma(s)$$

e,

$$\Gamma(s)\Gamma\left(s+\frac{1}{2}\right)=\frac{\sqrt{\pi}}{e^{2s-1}}\Gamma(2s).$$

Agora a equação funcional para a função zeta de Riemann:

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Resulta, por exemplo, da equação funcional, que $\zeta(0) = -1/2$.

Os zeros da função zeta são os seguintes:

(i) Zeros simples nos pontos $-2, -4, -6, \cdots$ que são chamados *zeros triviais.*

(ii) Zeros no domínio crítico, que é o conjunto dos números complexos s tais que $0 \leq Re(s) \leq 1$.

Com efeito, se $Re(s) > 1$, de acordo com o produto de Euler, $\zeta(s) \neq 0$. Se $Re(s) < 0$, então $Re(1 - s) > 1$, a expressão à direita da equação funcional não é nula e então os zeros de $\zeta(s)$ estão nos pontos $-2, -4, -6, \cdots$, que são exatamente os polos de $\Gamma(s/2)$.

O conhecimento dos zeros da função zeta no domínio crítico se traduz por um conhecimento mais profundo da distribuição dos números primos. A primeira coisa a observar é que os zeros no domínio crítico não são reais e que eles se colocam simetricamente em relação ao eixo real e também em relação à reta de equação $Re(s) = {}^{1}/_{2}$.

Riemann conjecturou que os zeros não triviais ρ da função zeta se encontram sobre a reta crítica $Re(s) = {}^{1}/_{2}$, quer dizer, $\rho = \frac{1}{2} + it$. Essa é a célebre *Hipótese de Riemann,* que até o momento não foi provada e sobre a qual varias generalizações já foram provadas. Note que esse problema é chamado de hipótese que tem uma conotação muito mais forte que uma conjectura que representa uma previsão do matemático sobre o modo que o mundo se comporta. Isso se dá devido à necessidade que muitos matemáticos tiveram para formular milhares de teoremas, pois se viram obrigados a pressupor a veracidade da previsão de Riemann para atingir seus próprios objetivos. Se a Hipótese de Riemann se transformar em um teorema, todos os resultados pendentes serão validados.

Riemann também teve a ideia de considerar todas as potências de números primos $p^n \leq x$, atribuindo a cada um desses números primos o peso $1/n$. Foi por ele definida a função:

$$J(x) = \begin{cases} \pi(x) + \frac{1}{2}\pi\left(x^{1/2}\right) + \frac{1}{3}\pi\left(x^{1/3}\right) + \frac{1}{4}\pi\left(x^{1/4}\right) + \cdots - \frac{1}{2m}, \\ quando\ x = p^m, onde\ m \geq 1\ e\ p\ é\ um\ número\ primo. \\ \pi(x) + \frac{1}{2}\pi\left(x^{1/2}\right) + \frac{1}{3}\pi\left(x^{1/3}\right) + \frac{1}{4}\left(\pi^{1/4}\right) + \cdots \\ quando\ x > 0\ é\ um\ número\ realque\ não\ é\ primo, \\ nem\ potência\ de\ número\ primo. \end{cases}$$

Uma das principais fórmulas conjecturadas por Riemann era uma expressão de $J(x)$ em função da integral logarítmica; essa fórmula faz intervir os zeros de $\zeta(s)$.

É preciso, em primeiro lugar, definir $Li(e^w)$, para todo número complexo $w = u + iv$, da maneira seguinte:

$$Li(e^w) = \int \frac{e^t}{t} dt + z$$

Onde a integral é calculada sobre a semirreta horizontal de $-\infty$ a $u + iv$ e $z = \pi i$, $-\pi i$ ou 0, segundo $v > 0, v < 0$ ou $v = 0$.

A fórmula de Riemann, provada por Von Mangoldt, é a seguinte:

$$J(x) = Li(x) - \sum_{\rho} Li(x^{\rho}) + \int_x^{\infty} \frac{dt}{t(t^2 - 1)\log t} - \log 2$$

em que o somatório é estendida a todos os zeros não triviais ρ de $\zeta(s)$, cada um contado com sua multiplicidade.

Seja:

$$R(x) = \sum_{m=1}^{\infty} \frac{\mu(m)}{m} Li\left(x^{1/m}\right),$$

função hoje chamada de Função de Riemann.

Riemann indicou a fórmula seguinte, que exprime $\pi(x)$ à custa da função $R(x)$:

$$\pi(x) = R(x) - \sum_{\rho} R(x^{\rho})$$

em que o somatório percorre todos os zeros ρ não triviais de $\zeta(s)$, cada um contado com a sua multiplicidade.

A Função de Riemann $R(x)$ dá uma excelente aproximação de $\pi(x)$. A expressão do erro utiliza os valores de $R(x^{\rho})$, para todas as raízes ρ de $\zeta(s)$ no domínio crítico.

Em 1893, Gram indicou a seguinte série de potências, que converge muito rapidamente, e permite calcular a função de Riemann:

$$R(x) = 1 + \sum_{n=1}^{\infty} \frac{1}{\pi\zeta(n+1)} x \frac{(\log x)^n}{n!}.$$

4.6. DE LA VALLÉE POUSSIN E HADAMARD

Riemann forneceu muitas ferramentas para a demonstração do *Teorema dos Números Primos* (RIBENBOIM, 2012):

$$\pi(x) \sim \frac{x}{\log x} \leftrightarrow \lim_{x\to\infty} \frac{\pi(x)}{x/_{logx}} = 1$$

Outras ferramentas foram obtidas da teoria das funções analíticas complexas, que passava por um período de grande desenvolvimento. O teorema foi provado por dois eminentes analistas de maneira independente e durante o mesmo ano de 1896. Eles foram: De La Valleé Poussin e Hadamard.

De La Valleé Poussin demonstrou a seguinte propriedade: existe $c > 0$ e $t_0 = t_0(c) > e^{2c}$, tais que $\zeta(s) \neq 0$ para todo $s = \sigma + it$ na região:

$$\begin{cases} 1 - \dfrac{c}{\log t_0} \leq \sigma \leq 1, & quando\ |t| \leq t_0 \\ 1 - \dfrac{c}{\log|t|} \leq \sigma \leq 1, & quando\ t_0 \leq |t| \end{cases}$$

Então, em particular, $\zeta(1+it) \neq 0$ para todo t, como fora provado por Hadamard.

A determinação de uma grande região onde a função $\zeta(s)$ não tem zeros foi um dos pontos importantes da demonstração do teorema dos números primos.

Hadamard e De La Valleé Poussin não se contentaram em demonstrar o Teorema dos Números Primos. Também calcularam o erro, mostrando que:

$$\pi(x) = Li(x) + O(xe^{-A\sqrt{\log x}}),$$

em que A é uma constante positiva.

Existem outras demonstrações do Teorema dos Números Primos com métodos analíticos. Entre elas, uma demonstração de Grosswald (1964) e outra, particularmente simples, deve-se a Newman (1980).

Existem outras formulações equivalentes do Teorema dos Números Primos. Utilizando a função de Tschebycheff, o teorema pode ser expresso assim:

$$\theta(x) \sim x.$$

Outra formulação faz intervir a função do somatório de Von Mangoldt. Seja:

$$\Lambda(n) = \begin{cases} \log p, & se\ n = p^{\nu}\ (\nu \geq 1) e\ p\ \text{é}\ primo, \\ 0, & nos\ demais\ casos. \end{cases}$$

Esta função aparece na expressão da derivada logarítmica da função zeta:

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}, \qquad para\ Re(s) > 1.$$

É também ligada à função $J(x)$:

$$J(x) = \sum_{n \leq x} \frac{\Lambda(n)}{\log n}.$$

A função somatório de $\Lambda(n)$ é definida por:

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

Ela se exprime, sem dificuldade, a partir da função de Tschebycheff:

$$\psi(x) = \theta(x) + \theta\left(x^{1/2}\right) + \theta\left(x^{1/3}\right) + \cdots.$$

O Teorema dos Números Primos também admite o enunciado equivalente seguinte:

$$\psi(x) \sim x.$$

4.7. ERDÖS E SELBERG

Acreditou-se durante muito tempo que métodos analíticos deviam ser empregados na demonstração do Teorema dos Números Primos. Houve grande surpresa na comunidade matemática, quando Erdös, assim como Selberg, em 1949, deu uma demonstração utilizando unicamente as estimativas elementares de certas funções aritméticas (RIBENBOIM, 2012).

Algumas dessas estimativas já eram conhecidas, como, por exemplo:

$$\sum_{p \le x} \frac{\log p}{p} = \log x + \gamma + O(1), \qquad \text{onde } \gamma \text{ é a constante de Euler,}$$

$$\sum_{n \le x} \frac{1}{n^{\sigma}} = \frac{x^{1-\sigma}}{1-\sigma} + \zeta(\sigma) + O\left(\frac{1}{x^{\sigma}}\right), \qquad onde\ \sigma > 1,$$

$$\sum_{n \le x} \log n = x\ \log x - x + O(\log x),$$

$$\sum_{n \le x} \frac{\log n}{n} = \frac{1}{2}(\log x)^2 + C + O\left(\frac{\log x}{x}\right).$$

As estimativas acima podem se obter utilizando as fórmulas de somatório de Abel, ou de Euler e MacLaurin e, de fato, não têm conteúdo aritmético.

As fórmulas a seguir, onde interveem números primos, são mais interessantes:

$$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1),$$

$$\sum_{p \le x} \frac{1}{p} = \log\log x + C + O\left(\frac{1}{\log x}\right), \qquad onde\ C = 0{,}2615\cdots,$$

$$\sum_{n\leq x}\frac{\Lambda(n)}{n}=\log x+O(1),$$

$$\sum_{n\leq x}\frac{\Lambda(n)\log n}{n}=\frac{1}{2}(\log x)^2+O(\log x).$$

Selberg deu, em 1949, a seguinte estimativa:

$$\sum_{p\leq x}(\log p)^2+\sum_{pq\leq x}(\log p)\,(\log q)=2x\log x+O(x),\qquad onde\ p,q\ são\ números\ primos.$$

Verdadeiramente, essa estimativa é equivalente a cada uma das duas seguintes:

$$\theta(x)\log x+\sum_{p\leq x}\theta\left(\frac{x}{p}\right)\log p=2x\log x+O(x),$$

$$\sum_{n\leq x}\Lambda(n)\log n+\sum_{mn\leq x}\Lambda(\mathrm{m})\Lambda(\mathrm{n})=2x\log x+O(x).$$

A partir dessas estimativas, Selberg pode dar uma demonstração elementar do Teorema dos Números Primos. Simultaneamente, Erdös apresentou, por um método elementar diferente, sua demonstração do Teorema dos Números Primos, utilizando a seguinte variante da estimativa de Selberg:

$$\frac{\psi(x)}{x}+\frac{1}{\log x}\sum_{n\leq x}\frac{\psi(x/n)}{x/n}\times\frac{\Lambda(n)}{n}=2+O\left(\frac{1}{\log x}\right).$$

Em 1970, Diamond e Steinig deram uma demonstração elementar com um erro explícito. Diamond (1982) escreveu um trabalho expositivo sobre os métodos elementares para a demonstração do Teorema dos Números Primos.

4.8. PRIMOS EM PROGRESSÃO ARITMÉTICA

Em 1837, Dirichlet demonstrou um teorema clássico:

Teorema de Dirichlet: Se $d \geq 2$ e $a \neq 0$ são inteiros primos entre si, então a progressão aritmética

$$a, a+d, a+2d, a+3d, \ldots$$

contém uma infinidade de números primos.

A demonstração usual deste teorema utilizando variáveis complexas pode ser encontrada em MARTINEZ; MOREIRA; SALDANHA; TENGAN, 2011.

Apresentamos a seguir a demonstração de um caso particular do teorema (MARTINEZ; MOREIRA; SALDANHA; TENGAN, 2011), utilizando o *polinômio ciclotômico* $\Phi_m(x)$ definido pela fórmula:

Função de Euler: Seja $\ell \in \{1, 2, \ldots\ldots, \ell, \ldots\ldots\ldots\}$

$\varphi(\ell)$ é o número de elementos do conjunto $\mathcal{S}$.

$$\mathcal{S} = \{\ell \in \mathbb{N} \,|1 \leq x \leq \ell | \; m.d.c.(x, \ell) = 1\}$$

Definição polinômio *ciclotômico* $\Phi_m(x)$

$\Phi_l(x) = \prod_{(k,l)=1}(x - \zeta^k)$ para $\zeta = e^{2\pi i/l}$

assim $\zeta^l = 1$

grau $\Phi_l(x) = \varphi(\ell)$ função Euler

$\prod_{l|m} \Phi_l(x) = x^m - 1$

Verifica-se facilmente que $\Phi_m(x)$ é o polinômio mônico de grau Φ_m cujas raízes são $\exp(2k\pi i/m), 0 \leq k < m, \; mdc(k, m) = 1$. Além disso $\Phi_m(x) \in \mathbb{Z}[x]$.

Caso particular do teorema de Dirichlet: Para todo inteiro positivo *d*, existem infinitos primos na progressão aritmética $S = \{dn + 1\}_{n \in \mathbb{N}}$.

Demonstração: Suponhamos que em S existe apenas um número finito de primos $p_1, \cdots, p_l$ e definamos $a = 2dp_1 \cdots p_l$. Seja q um divisor primo de $\Phi_d(a)$. Dado que $q|\Phi_d(a)| \; a^d - 1$, temos que $a^d \equiv 1(mod\ q)$. Mostremos que $d = ord_q a$. De fato, se $e = ord_q a$ é um divisor próprio de d, como o polinômio $(x^e - 1)\Phi_d(x)$ divide $x^d - 1$ então $a \bmod q$ será raiz dupla de $x^d - 1 \in \mathbb{Z}/(q)[x]$. Mas $q \mid a^d - 1$ e $d|a$ implica $q \nmid d$, assim todas as raízes de $x^d - 1$ são simples porque sua derivada dx^{d-1} só é nula em $x \equiv 0 \; (mod\ q)$, que não é raiz de $x^d - 1$. Portanto $d = ord_q a$ e assim $d|q - 1$, isto é, $q = nd + 1 \in S$, mas $q \neq p_j$pois $q|a^d - 1 \implies q \nmid a$, logo $q \notin S$, o que é uma contradição.

□

5. FUNÇÕES QUE DEFINEM OS NÚMEROS PRIMOS

Outro desafio imposto pelos números primos aos matemáticos de todos os tempos é definir funções que retornem números primos. Esse desafio se tornou mais premente após o desenvolvimento do método de criptografia RSA que requer dois números primos grandes.

Algumas fórmulas foram desenvolvidas, entretanto, ainda não se conhece uma fórmula simples para gerar números primos arbitrariamente grandes. As fórmulas existentes são tão complicadas que não ajudam muito nem a gerar números primos, nem a responder perguntas teóricas sobre a distribuição dos números primos.

RIBENBOIM (2012) classifica as fórmulas para gerar números primos em três grupos:

(A) Fórmulas em que: $f(n) = p_n$ (0 enésimo número primo)

(B) Fórmulas em que $f(n)$ é sempre um número primo e, se $n \neq m$, então $f(n) \neq f(m)$.

(C) Fórmulas onde o conjunto dos números primos é igual ao conjunto dos valores positivos da função.

Citaremos algumas das fórmulas existem a título de ilustração, sem nos preocuparmos com as demonstrações, devido à complexidade do tema.

5.1. FÓRMULA DE GANDHI

Em 1971, Gandhi descobriu a seguinte fórmula para gerar o enésimo número primo (RIBENBOIM, 2012):

$$p_n = \left\lfloor 1 - \frac{1}{\log 2} \log\left(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor$$

Onde:

- O símbolo $\lfloor x \rfloor$ indica o maior inteiro n tal que $n \leq x$ (x sendo um número real positivo).
- $P_{n-1} = p_1 p_2 \cdots p_{n-1}$
- $\mu(d)$ é a Função de Möbius, assim definida:

Uma forma equivalente de expressar a fórmula de Gandhi é: p_n é o único número inteiro tal que:

$$1 < 2^{p_n} \left(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) < 2.$$

Abaixo demonstração elaborada por Vanden Eynden em 1972.

Demonstração: Para simplificar a notação, seja $Q = P_{n-1}$, $p = p_n$ e $S = \sum_{d|Q} \frac{\mu(d)}{2^d - 1}$.

Então,

$$(2^Q - 1)S = \sum_{d|Q} \mu(d) \frac{2^Q - 1}{2^d - 1} = \sum_{d|Q} \mu(d)(1 + 2^d + 2^{2d} + \cdots + 2^{Q-d}).$$

Se $0 \leq t < Q$, o termo $\mu(d)2^t$ aparece exatamente quando d divide $mdc(t, Q)$. Então, o coeficiente de 2^t na soma é $\sum_{d|mdc(t,Q)} \mu(d)$; em particular, se $t = 0$, esse coeficiente é igual a $\sum_{d|Q} \mu(d)$.

□

Entretanto, para todo inteiro $m \geq 1$, é bem conhecido e fácil de demonstrar que:

$$\sum_{d|m} \mu(d) = \begin{cases} 1, & se\ m = 1 \\ 0, & se\ \ m > 1. \end{cases}$$

Se se escreve $\sum'_{0<t<Q}$ como a soma estendida a todos os valores de t tais que $0 < t < Q$ e $mdc(t, Q) = 1$, então $(2^Q - 1)S = \sum'_{0<t<Q} 2^t$; o maior índice t nessa soma é $t = Q - 1$. Daí resulta que:

$$2(2^Q - 1)\left(-\frac{1}{2} + S\right) = -(2^Q - 1) + \sum'_{0<t<Q} 2^{t+1} = 1 + \sum'_{0<t<Q-1} 2^{t+1}.$$

Se $2 \leq j < p_n = p$, existe um número primo q tal que $q < p_n = p$ (então q divide Q) e q divide $Q - j$. Cada um dos índices t, na soma considerada acima, satisfaz $0 < tQ - p$. Então:

$$\frac{2^{Q-p+1}}{2 \times 2^Q} < -\frac{1}{2} + S = \frac{1 + \sum'_{0<t\leq Q-p} 2^{t+1}}{2(2^Q - 1)} < \frac{2^{Q-p+2}}{2 \times 2^Q},$$

onde as desigualdades são fáceis de estabelecer.

Com uma multiplicação por 2^p, temos:

$$1 < 2^p\left(-\frac{1}{2} + 2\right) < 2.$$

□

5.2. PRIMOS DE MILLS

Outra fórmula para gerar números primos foi desenvolvida por Mills. Em 1947, ele provou que existe um número real $\theta > 0$ tal que para todo inteiro $n \geq 1$ o número $\lfloor \theta^{3^n} \rfloor$ é primo. Mills determinou que $\theta \sim 1{,}3064$ (RIBENBOIM, 2012).

Mais tarde demonstrou-se que se $c > 2{,}106$, existe um conjunto não enumerável de números reais $\theta > 0$ tais que para todo inteiro n o número $\lfloor \theta^{c^n} \rfloor$ é primo. Quando $c = 3$ o número θ indicado por Mills é o menor possível e é chamado constante de Mills.

Os números primos da forma $\lfloor \theta^{3^n} \rfloor$, onde θ é a constante de Mills, são chamados *primos de Mills*.

O valor da constante de Mills foi calculado com mais precisão, supondo a validade da Hipótese de Riemann, por Caldwell e Cheng em 2005: $\theta = 1{,}3063778838\cdots$ (com 61.684 algarismos).

Esta fórmula para gerar números primos não tem grande aplicação prática, pois as potências crescem muito rapidamente, além de ser conhecido apenas uma aproximação, ainda que bastante precisa, da constante de Mills.

Já se sabe que os números gerados pela fórmula de Mills com $n = 1, 2, 3 \cdots 10$ são números primos, sendo que quando $n = 10$ o número gerado tem 6.854 algarismos. Os números $\lfloor \theta^{3^{11}} \rfloor$ e $\lfloor \theta^{3^{12}} \rfloor$ foram calculados por P. Carmody e possuem 20.562 e 61.684 algarismos, respectivamente.

Outra fórmula similar de gerar números primos é:

$$p(n) = \left\lfloor 2^{2^{2^{\cdot^{\cdot^{\cdot^{2^w}}}}}} \right\rfloor, \text{com uma sucessão de } n \text{ expoentes}$$

Onde: $n \geq 1$

$$w \sim 1{,}9287800\cdots$$

Esta fórmula possui as mesmas limitações da fórmula de Mills, resultando em um número com mais de 5.000 algarismos quando $n = 4$.

6. CASOS PARTICULARES DE PRIMOS

6.1. NÚMEROS DE FERMAT GENERALIZADOS

Fermat conjecturou que todo número da forma $F_n = 2^{2^n} + 1$ era primo. Assim são chamados Números de Fermat, os números com tal formulação. Ele verificou sua conjectura até $n \leq 4$ e até este ponto, todos os números de Fermat são primos (MARTINEZ; MOREIRA; SALDANHA; TENGAN, 2011):

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65.537$$

O número seguinte, F_5, já é um número com 10 algarismos, o que impediu que Fermat testasse sua primariedade, visto que nesta época não havia tabelas de primos com números tão grandes.

Observe-se que $2^n + 1$ não é primo se n não é uma potência de 2: se p é um fator primo ímpar de n, podemos escrever

$$a^n + 1 = b^p + 1 = (b + 1)(b^{p-1} - b^{p-2} + \cdots + b^2 - b + 1).$$

Euler mostrou que todo fator primo de números F_n de Fermat (com $n \geq 2$) é da forma $k \times 2^{n+2} + 1$ e, testanto tais números conseguiu provar que 641 dividia F_5.

$2^{2^5} \equiv -1(641)$

$641 \equiv 5^4 + 2^4 = 2^7.5 + 1$

$5^4 \equiv -2^4.(641)$

$2^7 .5 \equiv -1\ (641)$

$2^{28}.\ 5^4 \equiv (-1)^4 \equiv 1\ (641)$

$-2^{32} \equiv 1\ (641)$

$(641) \mid 2^{32}+1$

De fato, temos: $F_5 = 4.294.967.297 = 641 \times 6.700.417$

Demonstração: Seja p um fator primo de F_n; então $2^{2^n} \equiv -1(mod\ p)$, daí $2^{2^{n+1}} \equiv 1\ (mod\ p)$ e assim, a ordem de $2\ módulo\ p$ é igual a 2^{n+1}; resulta que 2^{n+1} divide $p-1$, pelo pequeno Teorema de Fermat, em particular, 8 divide $p-1$. Assim, o símbolo de Legendre $2^{(p-1)/2} \equiv (2 \mid p) \equiv 1\ (mod\ p)$. Então 2^{n+1} divide $(p-1)/2$, o que mostra ser $p = k \times 2^{n+2} + 1$.

□

Já se demonstrou que F_n é composto para vários outros valores de n; nenhum outro primo de Fermat é conhecido. Até outubro de 2011 o menor número de Fermat que se desconhece se é primo ou composto é F_{33}, mas se conhecem muitos primos (alguns bastante grandes) da forma $a^{2^n} + 1$, que são conhecidos como *Primos de Fermat Generalizados*. O Teste de Pépin mostra como testar a primalidade de F_n.

Antes de apresentar este teste é necessário apresentar a seguinte proposição:

Proposição: Seja $n > 1$. Se para cada fator primo q de $n-1$ existe um inteiro a_q tal que ${a_q}^{n-1} \equiv 1(mod\ n)$ e ${a_q}^{(n-1)/q} \not\equiv 1(modn)$ então n é primo.

Demonstração: Seja q^{k_q} a maior potência de q que divide $n-1$. A ordem de a_q em $(\mathbb{Z}/(n))^x$ é um múltiplo de q^{k_q}, donde $\varphi(n)$ é um múltiplo de q^{k_q}. Como isto vale para todo fator primo q de $n-1$, $\varphi(n)$ é um múltiplo de $n-1$ e n é primo.

□

Teste de Pépin (MARTINEZ; MOREIRA; SALDANHA; TENGAN, 2011): Seja $F_n = 2^{2^n} + 1$; F_n é primo se, e somente se, $3^{(F_n-1)/2} \equiv -1\ (mod\ F_n)$.

Demonstração: Se $3^{(F_n-1)/2} \equiv -1\ (mod\ F_n)$ então a primalidade de $F_n$segue da proposição apresentada acima. Por outro lado, se F_n é primo então pelo critério de Euler e a lei de reciprocidade quadrática temos:

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

O Teste de Pepin é muito prático, mas se F_n é composto, o teste não dará qualquer fator de F_n. Desta forma, a fatoração de números de Fermat tem sido objeto de intensa exploração.

Em 1985, Dubner conseguiu descobrir números de Fermat generalizados bastante grandes que são primos, como por exemplo, $150^{2^{11}} + 1$. Em 202, Dubner e Gallot descreveram um método de computação para determinar a primariedade dos números de Mersenne.

Com esse processo, no fim de 2002, já haviam sido descobertos mais de 100 números de Fermat generalizados primos com mais de 100.000 algarismos. 46 números primos de Fermat generalizados são conhecidos com mais de 300.000. O maior entre eles tem mais de um milhão de organismos.

6.2. PRIMOS DE MERSENNE

Números da forma $M_p = 2^p - 1$, são conhecidos como números de Mersenne (MARTINEZ; MOREIRA; SALDANHA; TENGAN, 2011). Marin Mersenne foi um matemático, teórico musical, padre mínimo, teólogo e filósofo francês. Ficou conhecido sobretudo pelo seu estudo dos chamados primos de Mersenne. O asteróide 8191 Mersenne foi baptizado em sua honra (WIKIPÉDIA). Atualmente, os maiores números primos conhecidos são números de Mersenne. Os nove maiores números primos conhecidos até abril de 2010, são primos de Mersenne $M_p = 2^p - 1$ onde:

$$p = 43.112.609$$

$$p = 42.643.801$$

$$p = 37.156.667$$

$$p = 32.582.657$$

$$p = 30.402.457$$

$$p = 25.964.951$$

$$p = 24.036.583$$

$$p = 20.996.011$$

$$p = 13.466.917$$

Esses são os únicos primos conhecidos com mais de 4.000.000 algarismos.

Sabe-se, desde os tempos de Mersenne, que números desta forma podem ser primos ou compostos.

Por exemplo: $M_2 = 3,\ M_3 = 7,\ M_5 = 31,\ M_7 = 127$, são primos. Já, $M_{11} = 2.047 = 23 \times 89$, não é primo.

Em 1640, Mersenne afirmou que M_q é primo para $q = 13, 17, 19, 31, 67, 127\ e\ 257$. Em sua afirmação ele estava enganado em relação $q = 67\ e\ 257$, que são números compostos. Além disso, deixou de citar $q = 61, 89\ e\ 107$que são inferiores à 257 e também geram números primos de Mersenne. Apesar dos enganos cometidos, trata-se de um grande feito, tendo em vista a grandeza dos números envolvidos e poucos recursos computacionais da época.

O problema que se apresenta então é determinar se um determinado número de Mersenne é primo ou não e, neste caso, determinar seus fatores primos.

Parte do interesse em primos de Mersenne deve-se a sua estreita relação com os números perfeitos. Um número perfeito é um inteiro positivo que é igual à soma de seus divisores próprios.

Exemplos:

$$6 = 1 + 2 + 3$$

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

Números perfeitos pares são precisamente números da forma: $2^{p-1}(2^p - 1)$ onde $2^p - 1$ é um primo de Mersenne.

Pode-se demonstrar que $2^p - 1$ só pode ser primo quando p é primo.

Proposição: Se $2^n - 1$ é primo, então n é primo.

Demonstração: Se $n = ab$ com $a, b \geq 2$,

Então $1 < 2^a - 1 < 2^n - 1$ e

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \ (mod\ 2^a - 1)$$

e, $2^n - 1$ é composto. □

Em 1536, Hudalricus Regius mostrou que $2^p - 1$ não precisa ser primo sempre que p for primo. Como mostra o exemplo já citado anteriormente: $M_{11} = 2^{11} - 1 = 2.047 = 23 \times 89$.

Não se sabe demonstrar nem que existam infinitos primos de Mersenne, nem que existem infinitos primos p para os quais, M_p é composto. Conjectura-se que existam infinitos primos p para os quais M_p é primo e que, se p_n é o enésimo primo deste tipo, temos:

$$0 < A < \frac{\log p_n}{n} < B < +\infty$$

para constantes A e B.

Existem algumas conjecturas mais precisas quanto ao valor de

$$\lim_{n\to\infty} \sqrt[n]{p_n}\,.$$

Eberhart conjectura que este limite exista e seja igual a $3/2$; Wagstaff por outro lado conjectura que o limite seja:

$$2^{e^{-\gamma}} \approx 1{,}4757613971$$

onde γ é a constante de Euler-Mascheroni.

Mesmo quando M_p não é primo, podemos garantir que seus fatores primos serão especiais. Isso é muito útil quando procuramos primos de Mersenne, pois podemos eliminar alguns expoentes encontrando fatores primos de M_p. Isso também pode ser útil para conjecturarmos quanto à "probabilidade" de M_p ser primo, ou mais precisamente, quanto a distribuição dos primos de Mersenne.

Teorema de Reciprocidade Quadrática:

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

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

Proposição: Sejam $p > 2$ e q primos com q um divisor de M_p. Então $q \equiv 1\ (mod\ p)$e $q \equiv \pm 1\ (mod\ 8)$.

Demonstração: Se q divide M_p então $2^p \equiv 1\ (mod\ q)$, o que significa que a ordem de $2\ módulo\ q$ é p (pois p é primo). Isso significa que p é um divisor de $q-1$, ou seja, que $q \equiv 1\ (mod\ p)$. Por outro lado, $2 \equiv 2^{p+1} = \left(2^{(p+1)/2}\right)^2 (mod\ q)$, donde $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$ (Símbolo de Legendre) o que significa que $q \equiv \pm 1 (mod\ 8)$.

$$\left(\frac{a}{b}\right) = \begin{cases} 0, & \text{se } {}^{p}/_{a} \\ 1, & se\ a \equiv mod\ p \\ -1, & \text{caso contrário} \end{cases}$$

Os vários valores de p para os quais a primalidade de M_p foi testada sugerem que para a ampla maioria dos valores de p, M_p não é primo. Isso é apenas uma conjectura: não se saber sequer se existem infinitos primos p para os quais M_p seja composto. Vamos agora ver uma proposição que serve para garantir que para certos valores especiais de p, alguns muito grandes, M_p não é primo.

Proposição: Seja p primo, $p \equiv 3\ (mod\ 4)$. Então $2p+1$ é primo (p é primo de Sophie Germain) se, e somente se, $2p+1$ divide M_p.

Demonstração: Se $q = 2p+1$ é primo então:

$$M_p = 2^p - 1 = 2^{(q-1)/2} - 1 \equiv \left(\frac{2}{q}\right) - 1 (mod\ q).$$

Mas $p \equiv 3\ (mod\ 4)$ significa que $q \equiv 7\ (mod\ 8)$ donde $\left(\frac{2}{q}\right) = 1$. Assim, $M_p \equiv 0\ (mod\ q)$, o que demonstra uma das implicações da proposição.

Por outro lado, se $2p + 1$ não é primo, ele tem fatores primos r com $r \not\equiv 1\ (mod\ p)$ (pois $r < p$). Se $2p + 1$ dividisse M_p, r seria um fator primo de M_p, contrariando a proposição anterior.

□

O melhor método atualmente conhecido para saber se M_q é primo ou composto, repousa sobre o cálculo de uma sucessão recorrente indicada por Lucas (1878) e Lehmer (1930 e 1935). Entretanto, o método não permite determinar os fatores no caso de o número ser composto.

Teste de Primariedade para Números de Mersenne (RIBENBOIM, 2012): Sejam $P = 2$ e $Q = -2$; consideram-se as sucessões de Lucas $(U_m)_{m\geq 0}$ e $(V_m)_{m\geq 0}$ tendo parâmetros 2 e -2 e, consequentemente, discriminante $D = 12$. Então $N = M_n$ é primo se e somente se N divide $V_{(N+1)/2}$.

É desejável, para simplificar os cálculos, substituir a sucessão de Lucas $(V_m)_{m\geq 0}$ pela sucessão $(S_k)_{k\geq 0}$, que é definida, por recorrência, da seguinte maneira:

$$S_0 = 4, \qquad S_{k+1} = S_k^2 - 2$$

Assim, a sucessão começa pelos números $4, 14, 194, \cdots$. O teste pode ser formulado como se segue.

M_n é primo se e somente se M_n divide S_{n-2}.

Demonstração: $S_0 = 4 = V_2/2$. Supõe-se $S_{k-1} = V_{2^k}/2^{2^{k-1}}$; então

$$S_k = S_{k-1}^2 - 2 = \frac{V_{2^k}^2}{2^{2^k}} - 2 = \frac{V_{2^{k+1}} + 2^{2^k+1}}{2^{2^k}} - 2 = \frac{V_{2^{k+1}}}{2^{2^k}}.$$

De acordo com o teste, M_n é primo, se e somente se, M_n divide:

$$V_{(M_n+1)/2} = V_{2^{n-1}} = 2^{2^{n-2}} S_{n-2}.$$

Isso é, M_n divide S_{n-2}.

□

Com esse teste, Lucas mostrou em 1876 que M_{127} é um número primo e M_{67} é composto. Um pouco mais tarde, Pervushin mostrou que M_{61} é primo. Em 1927, Lehmer mostrou que M_{257} é composto.

6.3. PRIMOS GÊMEOS

Dizemos que p e q são *primos gêmeos* se p e q são primos e $|p - q| = 2$ (RIBENBOIM, 2012).

Conjectura-se que existem infinitos pares de primos gêmeos. Os menores números primos são: $(3, 5),\ (5, 7),\ (11, 13),\ (17, 19)$. Alguns primos gêmeos muito grandes são também conhecidos, como $65.516.468.355 \cdot 2^{333333} \pm 1$, que tem 100.355 dígitos cada um.

Os números primos gêmeos foram caracterizados por Clement em 1949, da seguinte maneira:

Seja $n \geq 2$. Os inteiros n e $n + 2$ são ambos primos, se e somente se:

$$4[(n-1)! + 1] + n \equiv 0\ (mod\ n + 2)$$

Demonstração: Se a congruência for satisfeita, então $n \neq 2{,}4$ e $(n-1)! + 1 \equiv 0\ mod\ n$ e, pelo Teorema de Wilson, n é primo. Por outro lado,

$$4(n-1)! + 2 \equiv 0\ (mod\ n + 2)$$

Que multiplicada por $n(n+1)$, dá:

$$[4(n+1)! + 1] + 2n^2 + 2n - 4 \equiv 0\ (mod\ n + 2)$$

E então:

$$4[(n+1)!+1]+(n+2)(2n-2) \equiv 0\ (mod\ n+2)$$

Logo:

$$(n+1)!+1 \equiv 0\ \ (mod\ n+2)$$

De acordo com o Teorema de Wilson, $n+2$ é também primo.

Reciprocamente, se n e $n+2$ são primos, então $n \neq 2$ e:

$$(n-1)!+1 \equiv 0\ (mod\ n),$$

$$(n+1)!+1 \equiv 0\ (mod\ n+2).$$

Ora, $n(n+1) = (n+2)(n-1)+2$ e daí $2(n-1)!+1 = k(n+2)$ onde k é inteiro. De $(n-1)! \equiv -1\ (mod n)$, resulta que $2k+1 \equiv 0\ (mod\ n)$ e, fazendo uma substituição,

$$4(n-1)!+2 \equiv -(n+2)\ (mod\ n(n+2))$$

E então:

$$4[(n-1)!+1]+n \equiv 0\ (mod\ n(n+2))$$

□

Entretanto, essa caracterização não tem qualquer interesse prático para determinar primos gêmeos.

O problema principal é decidir se existe uma infinidade de pares de primos gêmeos.

Para todo $x > 1$, seja $\pi_2(x)$ o número de primos p, tais que $p+2$ seja também primo e $p+2 \leq x$.

Brun anunciou em 1919 que existe um inteiro x_0, efetivamente calculável, tal que se $x \geq x_0$, então:

$$\pi_2(x) < \frac{100x}{(\log x)^2}.$$

A demonstração foi publicada em 1920.

Em outro artigo de 1919, Brun demonstrou o célebre resultado:

$$\sum\left(\frac{1}{p}+\frac{1}{p+2}\right)$$

Onde a soma é estendida a todos os primos p tais que $p+2$ também seja primo, é convergente, o que significa que, mesmo que existam infinitos pares de primos gêmeos, eles acabam por se afastar uns dos outros.

A soma:

$$B = \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots+\left(\frac{1}{p}+\frac{1}{p+2}\right)+\cdots$$

É chamada constante de Brun. Apoiando-se em considerações heurísticas sobre a distribuição dos primos gêmeos, essa constante foi calculada por Shanks e Wrench (1974), por Brent (1976) e mais recentemente por Nicely (2001) e por Sebah (2002), com o valor:

$$B = 1{,}90216051823\cdots$$

Brun também demonstrou que para todo $m \geq 1$, existem m primos sucessivos que não primos gêmeos.

A estimativa dada para $\pi_2(x)$ foi melhorada com a determinação da constante e do respectivo limite de erro. Isso foi executado, entre outros, por Bombieri e Davenport em 1966, através da aplicação do método do crivo.

Eis o resultado:

$$\pi_2(x) \leq 2C \prod_{p>2} \frac{p(p-2)}{(p-1)^2} \frac{x}{(\log x)^2}.$$

Hardy e Littlewood (1923) conjecturaram que a constante C seria igual a 1. Os melhores resultados obtidos até agora para a constante C foram:

$$C = 3{,}5 \quad \text{por Bombieri, Friedlander e Iwaniec (1986)}$$

$$C = 3{,}13 \quad \text{por S. Lou (não publicado)}$$

O produto infinito:

$$C_2 = \prod_{p>2} \frac{p(p-2)}{(p-1)^2}$$

é chamado a constante dos primos gêmeos e seu valor $0{,}66016\cdots$ foi calculado por Wrench em 1961.

6.4. PRIMOS DE SOPHIE GERMAIN

Sophie Germain provou o chamado primeiro caso do último Teorema de Fermat para os primos p para os quais $2p+1$ é primo. Por isso os primos que apresentam esta forma são chamados de primos de Sophie Germain. No dia 28 de junho de 1993, o matemático britânico Andrew Wiles fez a demonstração do teorema de Fermat também conhecido como o último Teorema de Fermat.

Sophie Germain demonstrou o seguinte teorema:

Se p e $2p+1$ são primos com $p>2$, então não existem inteiros x,y,z com $mdc(x,y,z)=1$ e $p \nmid xyz$ tais que $x^p+y^p+z^p=0$. Em outras palavras: o primeiro caso do último Teorema de Fermat é verdadeiro para todo expoente primo de Sophie Germain.

Demonstração: Observe inicialmente que $2p+1 \mid xyz$: caso contrário, pelo pequeno Teorema de Fermat, $x^{2p} \equiv 1 \pmod{2p+1}$, o que equivale a $(x^p-1)(x^p+1) \equiv 0\ (mod\ 2p+1)$. Assim, temos que $x^p \equiv \pm 1\ (mod\ 2p+1)$ e analogamente $y^p \equiv \pm 1\ (mod\ 2p+1)$ e $z^p \equiv \pm 1\ (mod\ 2p+1)$. Mas $x^p+y^p+z^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 (mod\ 2p+1)$, um absurdo.

□

Por outro lado temos,

$$(-x)^p = (y+z)(y^{p-1}-y^{p-2}z+\cdots-yz^{p-2}+z^{p-1})$$

Vamos mostrar que os dois fatores da direita são primos entre si. Se q é um primo que divide ambos os termos, então $y \equiv -z(mod\ q)$ e, portanto, $0 \equiv y^{p-1}-y^{p-2}z+\cdots+z^{p-1} \equiv py^{p-1}\ (mod\ q)$; temos $q \neq p$ pois $q \mid x$, assim $q \mid py^{p-1} \Longrightarrow q \mid y$, mas então $z \equiv -y \equiv$

$0\ (mod\ q)$ e q dividiria simultaneamente x, y, z, contrariando a hipótese $mdc(x, y, z) = 1$. Assim, pela fatoração única em primos existem inteiros a, d tais que:

$$a^p = y + z \quad \text{e} \quad d^p = y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1}$$

e analogamente:

$$b^p = x + z \quad \text{e} \quad e^p = x^{p-1} - x^{p-2}z + \cdots - xz^{p-2} + z^{p-1}$$

$$c^p = x + y \quad \text{e} \quad f^p = x^{p-1} - x^{p-2}y + \cdots - xy^{p-2} + y^{p-1}$$

para b, c, e, f inteiros.

Como $2p + 1 \mid xyz$, podemos supor sem perda de generalidade que $2p + 1 \mid x$. Assim, de $2x = b^p + c^p - a^p$, temos que $2p + 1 \mid b^p + c^p - a^p$ e o mesmo argumento no início da demonstração mostra que $2p + 1 \mid abc$ também.

Mas se $2p + 1 \mid b = x + z$ ou $2p + 1 \mid c = x + y$, como $2p + 1 \mid x$ e $x^p + y^p + z^p = 0$ teríamos que $2p + 1 \mid mdc(x, y, z) = 1$, um absurdo.

Por outro lado, temos $f^p \equiv y^{p-1}(mod\ 2p + 1)$ e se $2p + 1 \mid a$, então $2p + 1 \nmid d$ e $y \equiv -z\ (mod\ 2p + 1) \Longrightarrow d^p \equiv py^{p-1} (\mathrm{mod}\ 2\mathrm{p} + 1)$.

Assim, $2p + 1 | f$, pois caso contrário teríamos:

$$\pm p \equiv pf^p \equiv py^{p-1} \equiv d^p \equiv \pm 1\ (\mathrm{mod}\ 2\mathrm{p} + 1)$$

Um absurdo.

Mas neste caso, $2p + 1 \mid z$ também, o que é impossível já que $mdc\ (x, y, z) = 1$, completando a prova.

Conjectura-se a existência de uma infinidade de primos de Sophie Germain, porém sua demonstração pode ser tão difícil quanto à da existência de uma infinidade de primos gêmeos.

O teorema de Sophie Germain foi estendido por Legendre e Dénes (1951) e mais recentemente, por Fee e Grandville (1991).

A estimativa do número de primos de Sophie Germain inferiores a um número $x \geq 1$ é dada por $\pi_{SG}(x)$:

$$\pi_{SG}(x) < \frac{C\ x}{(\log x)^2}.$$

Acredita-se que $\pi_{SG}(x)$ seja assintótico a $\frac{C\ x}{(\log x)^2}$ para algum $c > 0$, mas como dito, não se sabe demonstrar sequer a existência de infinito primos de Sophie Germain.

7. CONCLUSÃO

Este trabalho nos revela o fascínio provocado pelos números primos em acadêmicos ao longo de toda a história da matemática. Este fascínio não é um acaso, como vimos, trata-se de um tema profundamente complexo e instigante que vem desafiando a comunidade científica há séculos. Sua aplicação em criptografia RSA, que viabiliza diariamente milhares de transações financeiras via internet, torna o tema ainda mais discutido em diversos campos de estudo e com os mais diversos interesses, incluindo desde aqueles que buscam garantir e aprimorar a segurança do sistema, como os que buscam suas fragilidades para uso menos nobres.

Diante de sua complexidade, o tema é abordado de forma superficial tanto no ensino médio quanto no ensino superior de Matemática. O que é plenamente compreendido pela necessidade de conhecimento de Matemática Avançada para maior aprofundamento. Entretanto, a literatura já registra algumas tentativas de simplificar o tema de forma a torna-lo compreensível a alunos com poucos ou nenhum conhecimento de matemática avançada, sendo por tanto, um tema bastante interessante para futuros trabalhos de monografia para professores de matemática.

8. REFERÊNCIAS

ÁVILA, Geraldo Severo de Souza. **Várias Faces da Matemática**: Tópicos para licenciatura e leitura geral. São Paulo: Blucher, 2010.

DU SAUTOY, Marcus. **A Música dos Números Primos**: A história de um problema não resolvido na matemática. Rio de Janeiro: Zahar, 2007.

FARIAS, Fernando de. **Uma análise comparativa entre os testes de primalidade AKS e Miller-Rabin.** Monografia (Conclusão de curso). Universidade Católica de Brasília Curso de Matemática

IRELAND, Kenneth; ROSEN, Michael. **A Classical Introduction to Modern Number Theory.** 1972, 1982, 1980 Springer Verlag New York, Inc.

MARTINEZ, Fábio Brochero; MOREIRA, Carlos Gustavo; SALDANHA, Nicolau; TENGAN, Eduardo. **Teoria dos Números**: Um passeio com primos e outros números familiares pelo mundo inteiro. Rio de Janeiro: IMPA, 2011.

MOREIRA, Carlos Gustavo; SALDANHA, Nicolau. **Primos de Mersene** (e outros primos muito grandes). Rio de Janeiro: IMPA, 2008.

RIBENBOIM, Paulo. **Números Primos**: Velhos mistérios e novos recordes. Rio de Janeiro: IMPA, 2012.

SANTOS, José Plínio de Oliveira. **Teoria dos Números**. Rio de Janeiro: IMPA, 2011.

WEIL, André. **Basic Number Theory.** New York: Heidelberg, Berlin, 1974.